Safety Reference Manual

Allen-Bradley

GuardLogix 5570 Controller Systems

Catalog Numbers 1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT, 1756-L7SP, 1756-L7SPXT, 1756-L72EROMS,
Studio 5000 Logix Designer Applications

Original Instructions

Allen-Bradley • Rockwell Software

Rockwell Automation

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

	**WARNING:** Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.
	**ATTENTION:** Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.
IMPORTANT	Identifies information that is critical for successful application and understanding of the product.

Labels may also be on or inside the equipment to provide specific precautions.

	**SHOCK HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.
	**BURN HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.
	**ARC FLASH HAZARD:** Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

This manual contains new and updated information. Changes throughout this revision are marked by change bars, as shown to the right of this paragraph.

New and Updated Information

This table contains the changes made in this revision.

Topic	Page
Added Kinetix® 5700 servo drive user manual and PowerFlex® 527 AC drive user manuals to the Additional Resources	10
Added Kinetix 5700 Servo Drives and PowerFlex 527 Adjustable Frequency AC Drives to list of GuardLogix® system components	16
Added information to the table of GuardLogix system components to identify which versions of RSLogix™ 5000 software support 1756-L61S, 1756-L62S, 1756-L63S, 1756-LSP, 1768-L43S, and 1768-L45S controllers and that those controllers are not supported in the Studio 5000 Logix Designer™ application.	16
Updated ControlNet illustration	24
Added Kinetix 5700 Servo Drives User Manual and PowerFlex 527 Adjustable Frequency AC Drives User Manual to the important statement about using Motion Direct Commands	72

Notes:

Chapter 4

CIP Safety and the Safety Network Number

Chapter 5

Characteristics of Safety Tags, the Safety Task, and Safety Programs

Chapter 6

Safety Application Development

This manual is intended to describe the GuardLogix 5570 controller system, which is **type-approved** and certified for use in safety applications up to and including SIL CL 3 according to IEC 61508 and IEC 62061, safety applications up to and including Performance Level PLe (Category 4) according to ISO 13849-1.

Use this manual if you are responsible for the development, operation, or maintenance of a GuardLogix 5570 controller-based safety system that uses the Studio 5000 Logix Designer™ application, version 21.000 or later. You must read and understand the safety concepts and the requirements that are presented in this manual before operating a GuardLogix 5570 controller-based safety system.

For safety requirements related to GuardLogix 5570 controllers in RSLogix 5000 projects, refer to the GuardLogix Controllers Safety Reference Manual, publication 1756-RM093.

Studio 5000 Environment

The Studio 5000 Automation Engineering & Design Environment™ combines engineering and design elements into a common environment. The first element in the Studio 5000® environment is the Logix Designer application. The Logix Designer application is the rebranding of RSLogix 5000 software and continues to be the product to program Logix5000™ controllers for discrete, process, batch, motion, safety, and drive-based solutions.

The Studio 5000 environment is the foundation for the future of Rockwell Automation® engineering design tools and capabilities. The Studio 5000 environment is the one place for design engineers to develop all elements of their control system.

Terminology

The following table defines terms that are used in this manual.

Table 1 - Terms and Definitions

Abbreviation	Full Term	Definition
1oo2	One out of Two	Identifies the programmable electronic controller architecture.
CIP	Common Industrial Protocol	An industrial communication protocol that is used by Logix5000-based automation systems on EtherNet/IP™, ControlNet™, and DeviceNet™ communication networks.
CIP Safety	Common Industrial Protocol – Safety Certified	SIL 3 -rated version of CIP.
DC	Diagnostic Coverage	The ratio of the detected failure rate to the total failure rate.
EN	European Norm.	The official European Standard.
GSV	Get System Value	A ladder logic instruction that retrieves specified controller status information and places it in a destination tag.
PC	Personal computer	Computer that is used to interface with, and control, a Logix-based system via the Studio 5000 environment.
PFD	Probability of Failure on Demand	The average probability of a system to fail to perform its design function on demand.
PFH	Probability of Failure per Hour	The probability of a system to have a dangerous failure occur per hour.
PL	Performance Level	ISO 13849-1 safety rating.
SNN	Safety Network Number	A unique number that identifies a section of a safety network.
SSV	Set System Value	A ladder logic instruction that sets controller system data.
--	Standard	Any object, task, tag, program, or component in your project that is not a safety-related item (that is, standard controller refers generically to a ControlLogix® or CompactLogix™ controller).

Additional Resources

These documents contain more information about related products from Rockwell Automation.

Resource	Description
GuardLogix 5570 Controllers User Manual, publication 1756-UM022	Provides information on how to install, configure, program, and use GuardLogix 5570 controllers in Studio 5000 Logix Designer projects
GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Provides information on the GuardLogix Safety Application instruction set
Guard I/O™ DeviceNet Safety Modules User Manual, publication 1791DS-UM001	Provides information on how to use Guard I/O DeviceNet safety modules
Guard I/O EtherNet/IP Safety Modules User Manual, publication 1791ES-UM001	Provides information on how to use Guard I/O EtherNet/IP safety modules
POINT Guard I/O Safety Modules User Manual, publication 1734-UM013	Provides information on how to install and use POINT Guard I/O™ modules
Kinetix 5500 Servo Drives User Manual, publication 2198-UM001	Provides information on how to install and use Kinetix 5500 servo drives
Kinetix 5700 Servo Drives User Manual, publication 2198-UM002	Provides information on how to install and use Kinetix 5700 servo drives
PowerFlex 527 Adjustable Frequency AC Drive User Manual, publication 520-UM002	Provides information on how to install and use PowerFlex 527 drives
Using ControlLogix in SIL 2 Applications Safety Reference Manual, publication 1756-RM001	Describes requirements for using ControlLogix controllers, and GuardLogix standard task, in SIL 2 safety control applications
Logix5000 General Instruction Set Reference Manual, publication 1756-RM003	Provides information on the Logix5000 Instruction Set
Logix Common Procedures Programming Manual, publication 1756-PM001	Provides information on programming Logix5000 controllers, including how to manage project files, organize tags, program and test routines, and handle faults
Logix5000 Controllers Add-On Instructions Programming Manual, publication 1756-PM010	Provides information on how to create and use standard and safety Add-On Instructions in Logix applications

Resource	Description
ControlLogix System User Manual, publication 1756-UM001	Provides information on how to use ControlLogix controllers in nonsafety applications
DeviceNet Modules in Logix5000 Control Systems User Manual, publication DNET-UM004	Provides information on how to use the 1756-DNB module in a Logix5000 control system
EtherNet/IP Modules in Logix5000 Control Systems User Manual, publication ENET-UM001	Provides information on how to use the 1756-ENBT module in a Logix5000 control system
ControlNet Modules in Logix5000 Control Systems User Manual, publication CNET-UM001	Provides information on how to use the 1756-CNB module in Logix5000 control systems
Logix5000 Controllers Execution Time and Memory Use Reference Manual, publication 1756-RM087	Provides information on estimating the execution time and memory use for instructions
Logix Import Export Reference Manual, publication 1756-RM084	Provides information on how to use he Logix Designer Import/Export utility
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system
Product Certifications website, http://www.ab.com	Provides declarations of conformity, certificates, and other certification details

You can view or download publications at http://www.rockwellautomation.com/literature/. To order paper copies of technical documentation, contact your local Allen-Bradley distributor or Rockwell Automation sales representative.

Notes:

Safety Integrity Level (SIL) Concept

SIL 3 Certification

GuardLogix 5570 controller systems are type-approved and certified for use in safety applications up to and including SIL CL3 according to IEC 61508 and IEC 62061, safety applications up to and including Performance Level PLe (Category 4) according to ISO 13849-1. SIL requirements are based on the standards current at the time of certification.

IMPORTANT When the GuardLogix controller is in Run or Program mode and you have not validated the application program, you are responsible for maintaining safe conditions.

In addition, the standard tasks within GuardLogix controllers can be used either for standard applications or SIL 2 safety applications as described in the Using ControlLogix in SIL 2 Applications Reference Manual, publication 1756-RM001. In either case, do not use SIL 2 or standard tasks and variables to build up safety loops of a higher level. The safety task is the only task that is certified for SIL 3 applications.

Use the Studio 5000 Logix Designer application to create programs for GuardLogix 5570 controllers.

The TÜV Rheinland has approved GuardLogix 5570 controller systems for use in safety-related applications up to SIL CL 3, in which the de-energized state is considered to be the safe state. All examples that are related to I/O included in this manual are based on achieving de-energization as the safe state for typical Machine Safety and Emergency Shutdown (ESD) Systems.

IMPORTANT As the system user, you are responsible for the following:

- The setup, SIL rating, and validation of any sensors or actuators that are connected to the GuardLogix system
- Project management and functional test
- Access control to the safety system, including password handling
- Programming the application and the device configurations in accordance with the information in this safety reference manual and the GuardLogix 5570 Controllers User Manual, publication 1756-UM022

When applying Functional Safety, restrict access to qualified, authorized personnel who are trained and experienced. The safety-lock function, with passwords, is provided in the Logix Designer application.

For information on how to use the safety-lock feature, refer to the GuardLogix 5570 Controllers User Manual, publication 1756-UM022.

Proof Tests

IEC 61508 requires you to perform various proof tests of the equipment that is used in the system. Proof tests are performed at user-defined times. For example, proof test intervals can be once a year, once every 15 years, or whatever time frame is appropriate.

GuardLogix 5570 controllers have a proof test interval of up to 20 years. Other components of the system, such as safety I/O devices, sensors, and actuators can have shorter proof test intervals. Include the controller in the functional verification testing of the other components in the safety system.

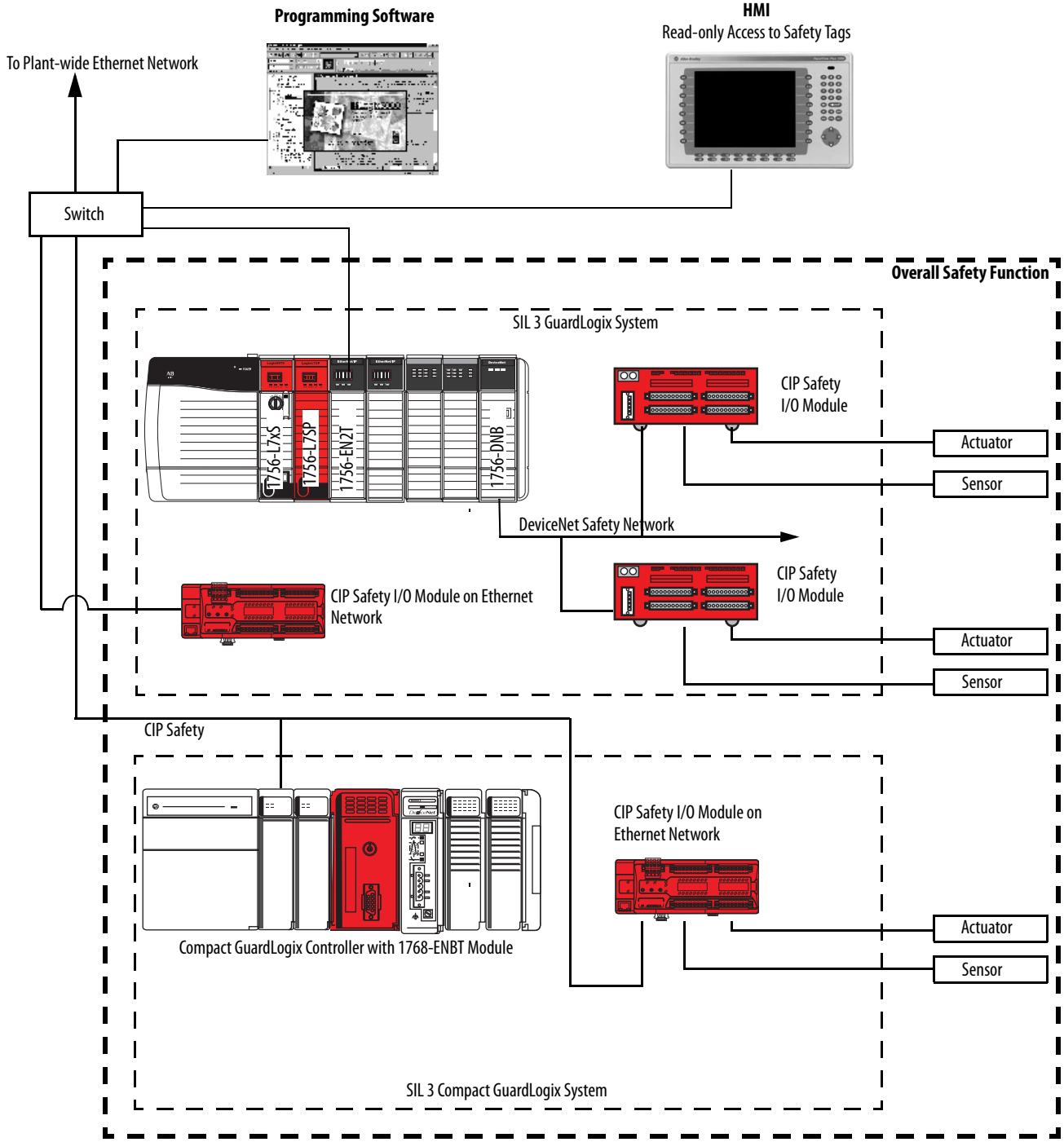
IMPORTANT Your specific applications determine the time frame for the proof test interval. However, this is mainly related to safety I/O devices and field instrumentation.

GuardLogix Architecture for SIL 3 Applications

The following illustration shows a typical SIL function, including the following:

- The overall safety function
- The GuardLogix portion of the overall safety function
- How other devices (for example, HMI) are connected, while operating outside the function

Figure 1 - Typical SIL Function



GuardLogix System Components

The tables in this section list SIL 3-certified GuardLogix components and non-SIL 3-certified components that can be used with SIL 3 GuardLogix systems.

For the most current list of GuardLogix controller and CIP Safety I/O devices certified series and firmware versions, see http://www.rockwellautomation.com/products/certification/safety/. firmware versions are available at http://support.rockwellautomation.com/ControlFLASH™/.

Table 2 - SIL 3-certified GuardLogix Components

Device Type	Cat. No.	Description	Related Documentation[3]	
			Installation Instructions	User Manual
1756 GuardLogix primary controller (ControlLogix5570S)	1756-L71S	Controller with 2 MB standard, 1 MB safety memory	N/A[4]	• With Studio 5000 environment, version 21 or later: 1756-UM022 • With RSLogix 5000 software, version 20 and earlier: 1756-UM020
	1756-L72S	Controller with 4 MB standard, 2 MB safety memory		
	1756-L73S	Controller with 8 MB standard, 4 MB safety memory		
	1756-L73SXT	Controller (XT) with 8 MB standard, 4 MB safety memory		
1756 GuardLogix safety partner (ControlLogix557SP)	1756-L7SP	Safety partner		
	1756-L7SPXT	Safety partner (XT)		
1756 GuardLogix primary controller (ControlLogix5560S)[1]	1756-L61S	Controller with 2-MB standard, 1 MB safety memory	N/A[4]	1756-UM020
	1756-L62S	Controller with 4-MB standard, 1 MB safety memory		
	1756-L63S	Controller with 8-MB standard, 3.75 MB safety memory		
1756 GuardLogix safety partner (ControlLogix55SP)[1]	1756-LSP	Safety partner		
1768 Compact GuardLogix Controller (CompactLogix4xS)[2]	1768-L43S	Controller with support for two 1768 modules	N/A[4]	1768-UM002
	1768-L45S	Controller with support for four 1768 modules		
CIP Safety I/O modules on DeviceNet networks	For the most current list of certified series and firmware versions, see the safety certificate at http://www.rockwellautomation.com/products/certification/safety/		1791DS-IN001 1791DS-IN002 1732DS-IN001	1791DS-UM001
CIP Safety I/O modules on EtherNet/IP networks			1791ES-IN001	1791ES-UM001
POINT Guard I/O modules			N/A[4]	1734-UM013
Kinetix 5500 servo drives (catalog numbers that end in -ERS2)	For the most current list of certified series and firmware versions, see the safety certificate at http://www.rockwellautomation.com/products/certification/safety/		2198-IN001	2198-UM001
Kinetix 5700 servo drives	For the most current list of certified series and firmware versions, see the safety certificate at http://www.rockwellautomation.com/products/certification/safety/			2198-UM002
PowerFlex 527 Adjustable Frequency AC Drives	For the most current list of certified series and firmware versions, see the safety certificate at http://www.rockwellautomation.com/products/certification/safety/			520-UM002

(1) Certified for use with RSLogix 5000 software, version 14, and versions 16 through 20. 1756-L61S, 1756-L62S, 1756-L63S and 1756-LSP controllers are not supported in the Studio 5000 Logix Designer application.

(2) Certified for use with RSLogix 5000 software, versions 18 through 20. 1768-L43S and 1768-L45S controllers are not supported in the Studio 5000 Logix Designer application.

(3) These publications are available from Rockwell Automation by visiting http://www.rockwellautomation.com/literature.

(4) See user manual for installation instructions.

Table 3 - Components Suitable for Use with 1756 GuardLogix Controller Safety Systems

Device Type	Cat. No.	Description	Series[1]	Revision[1]	Related Documentation[3]	
					Installation Instructions	User Manual
Chassis	1756-A4 1756-A7 1756-A10 1756-A13 1756-A17	4-slot chassis 7-slot chassis 10-slot chassis 13-slot chassis 17-slot chassis	B	N/A	1756-IN005	N/A
	1756-A4LXT 1756-A5XT 1756-A7XT 1756-A7LXT	4-slot XT chassis 5-slot XT chassis 7-slot XT chassis 7-slot XT chassis	B	N/A		
Power supply	1756-PA72	Power supply, AC	C	N/A	1756-IN005	N/A
	1756-PB72	Power supply, DC	C			
	1756-PA75	Power supply, AC	B			
	1756-PB75	Power supply, DC	B			
	1756-PAXT	XT power supply, AC	B			
	1756-PBXT	XT power supply, DC	B			
Communication modules	1756-ENBT 1756-EN2T 1756-EN2F 1756-EN2TR 1756-EN3TR	EtherNet/IP bridge	A A A C B	3.006 2.005 2.005 10.007 10.007	ENET-IN002	ENET-UM001
	1756-EN2TXT 1756-EN2TRXT	XT EtherNet/IP bridge (copper)	C C	5.007 10.006		
	1734-AENT	POINT I/O™ Ethernet adapter	A	3.001	1734-IN590	1734-UM011
	1756-DNB	DeviceNet bridge	A	6.002	DNET-IN001	DNET-UM004
	1756-CN2	ControlNet bridge	A	12.001	CNET-IN005	CNET-UM001
	1756-CN2R	ControlNet bridge, redundant media	A	12.001		
	1756-CN2RXT	XT ControlNet bridge, redundant media	B	20.020		
Programming software	9324-*xxxx*	RSLogix 5000 software for GuardLogix 5560 controllers	N/A	14[2]	N/A	Consult online help.
		RSLogix 5000 software for GuardLogix 5570 (XT) controllers		20		
	9324-*xxxx*	Studio 5000 environment for GuardLogix 5570 (XT) controllers		21		
Memory cards	1784-CF128	128 MB CompactFlash Card for GuardLogix 5560 controllers	N/A	N/A	N/A	N/A
	1784-SD1	1 GB Secure Digital (SD) Card for GuardLogix 5570 controllers				
	1784-SD2	2 GB Secure Digital (SD) Card for GuardLogix 5570 controllers				

(1) This version or later.

(2) RSLogix 5000 software, version 15, does not support GuardLogix safety controllers.

(3) These publications are available from Rockwell Automation by visiting http://www.rockwellautomation.com/literature.

You can fill slots of a SIL 3 system chassis that are not used by the GuardLogix SIL 3 system with other ControlLogix (1756) modules that are certified to the Low Voltage and EMC Directives.

IMPORTANT ControlLogix-XT™ system components are rated for extreme environmental conditions only when used properly with other Logix-XT system components. The use of ControlLogix-XT components with traditional ControlLogix or GuardLogix system components nullifies extreme environment ratings.

To find the certificates for the 'Programmable Control–ControlLogix Product Family', refer to http://www.rockwellautomation.com/products/certification/ce/.

GuardLogix Certifications

The ControlLogix Controllers Technical Data, publication 1756-TD001, lists the product specifications and the agency certifications for which the products are approved. If a product has achieved agency certification, it is marked as such on the product labeling. See the Product Certification link at http://www.rockwellautomation.com/products/certification/ for Declarations of Conformity, Certificates, and other certification details.

GuardLogix PFD and PFH Specifications

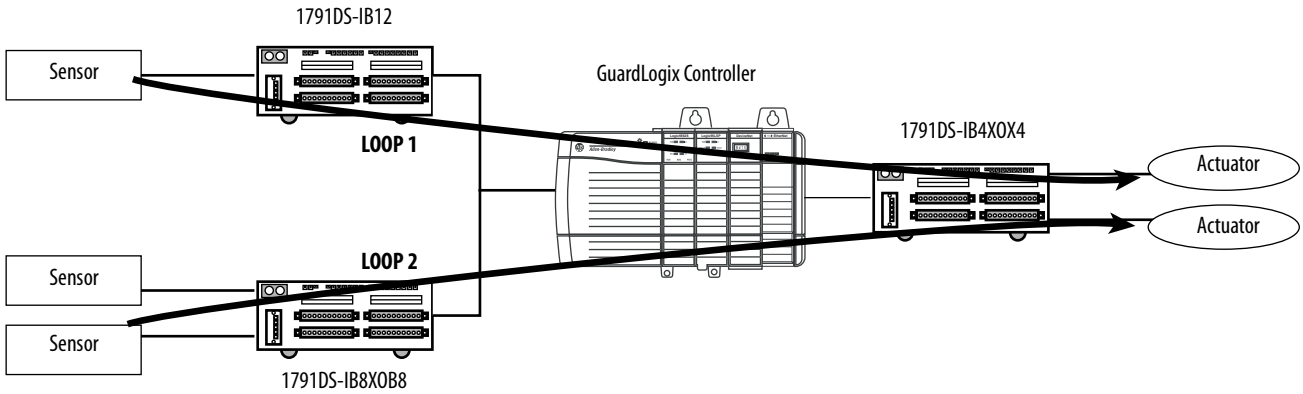
Safety-related systems can be classified as operating in either a Low Demand mode, or in a High Demand/Continuous mode. IEC 61508 quantifies this classification by stating that the frequency of demands for operation of the safety system is no greater than once per year in the Low Demand mode, or greater than once per year in High Demand/Continuous mode.

The Safety Integrity Level (SIL) value for a Low Demand safety-related system is directly related to order-of-magnitude ranges of its average probability of failure to satisfactorily perform its safety function on demand or, simply, probability of failure on demand (PFD). The SIL value for a High Demand/Continuous mode safety-related system is directly related to the probability of a dangerous failure occurring per hour (PFH).

PFD and PFH values are associated with each of the three primary elements that constitute a safety-related system (the sensors, the logic element, and the actuators). Within the logic element, you also have input, processor, and output elements.

For PFD and PFH values and proof test intervals for Guard I/O modules, see Appendix E, GuardLogix Systems Safety Data.

Figure 2 - PFH Example



To determine the logic element PFH for each safety loop in the simple example system that is shown in the PFH Example, sum the PFH values for each component in the loop. The PFH Equations by Safety Loop table provides a simplified example of PFH value calculations for each safety loop that is shown in the PFH Example illustration.

Table 4 - PFH Equations by Safety Loop

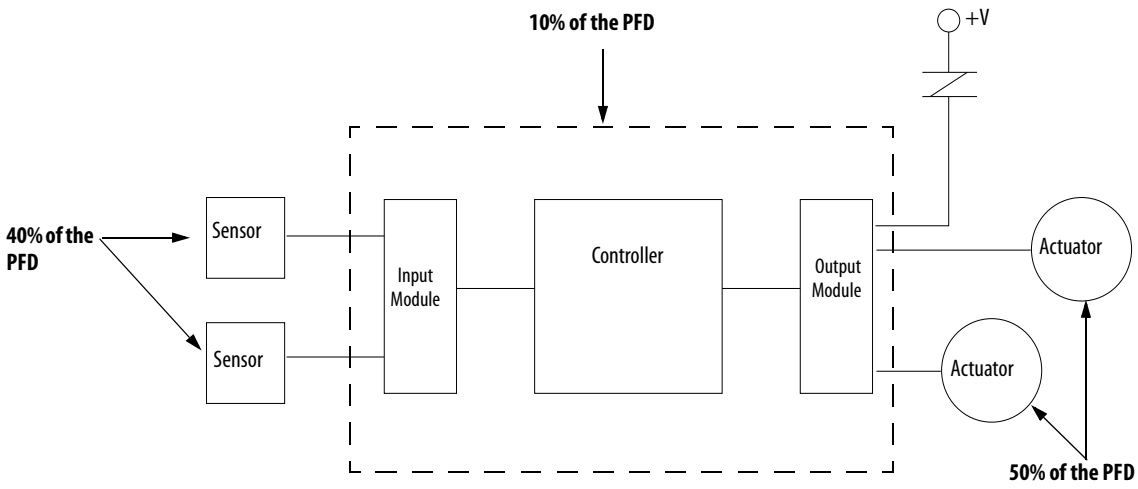
For This Loop	Sum the PFH Values of These Components
Total PFH for loop 1 =	1791DS-IB12 + GuardLogix controller + 1791DS-IB4X0X4
Total PFH for loop 2 =	1791DS-IB8X0B8 + GuardLogix controller + 1791DS-IB4X0X4

When calculating PFH values, you must take into account the specific requirements of your application, including test intervals.

Safety Integrity Level (SIL) Compliance Distribution and Weight

The GuardLogix controller and I/O system can conservatively be assumed to contribute 10% of the reliability burden. A SIL 3 system may need to incorporate multiple inputs for critical sensors and input devices, as well as dual outputs connected in series to dual actuators dependent on SIL assessments for the safety-related system.

Figure 3 - Reliability Burden



System Reaction Time

The system reaction time is the amount of time from a safety-related event as an input to the system until the system sets corresponding outputs to their safe state. Faults within the system can also affect the reaction time of the system. The system reaction time is the sum of the following reaction times.

Each of the reaction times is variably dependent on factors such as the type of I/O device and instructions that are used in the program.

Safety Task Reaction Time

The safety-task reaction time is the worst-case delay from any input change that is presented to the controller until the processed output is set by the output producer. It is less than or equal to the sum of the safety task period and the safety task watchdog.

Safety Task Period and Safety Task Watchdog

The safety task period is the interval at which the safety task executes.

The safety-task watchdog time is the maximum permissible time for safety task processing. If safety-task processing time exceeds the safety-task watchdog time, a nonrecoverable safety fault occurs in the controller and outputs transition to the safe state (off) automatically.

You define the safety-task watchdog time, which must be less than or equal to the safety task period.

The safety-task watchdog time is set in the task properties window of the Logix Designer application. This value can be modified online, regardless of controller mode, but it cannot be changed when the controller is safety-locked or once a safety task signature is created.

Contact Information If Device Failure Occurs

If you experience a failure with any SIL 3-certified device, contact your local Allen-Bradley distributor to initiate the following actions:

- You can return the device to Rockwell Automation so the failure is appropriately logged for the catalog number that is affected and a record is made of the failure.
- You can request a failure analysis (if necessary) to try to determine the cause of the failure.

GuardLogix Controller System

For a brief listing of components suitable for use in Safety Integrity Level (SIL) 3 applications, see the table on page 16. For more detailed and up-to-date information, see http://www.rockwellautomation.com/products/certification/safety/.

When installing a GuardLogix 5570 controller, follow the information in the GuardLogix 5570 Controllers User Manual, publication 1756-UM022.

GuardLogix 5570 Controller Hardware

The GuardLogix controller consists of a primary controller (ControlLogix 557*x*S) and a safety partner (ControlLogix 557SP). These two modules work in a 1oo2 architecture to create the SIL 3-capable controller. They are described in the following sections.

Both the primary controller and safety partner perform power-up and runtime functional-diagnostic tests of all safety-related components in the controller.

For details on status indicator operation, refer to the GuardLogix 5570 Controllers User Manual, publication 1756-UM022.

IMPORTANT	Status indicators are not reliable indicators for safety functions. Use them only for general diagnostics during commissioning or troubleshooting. Do not attempt to use status indicators to determine operational status.

For a list of GuardLogix safety controller catalog numbers, see Table 2 on page 16. For a list of standard ControlLogix components suitable for safety applications, see Table 3 on page 17.

Primary Controller

The primary controller is the processor that performs standard and safety control functions and communicates with the safety partner for safety-related functions in the GuardLogix control system. The primary controller consists of a central processor, I/O interface, and memory.

Safety Partner

To satisfy SIL 3 requirements, a safety partner must be installed in the slot immediately to the right of the primary controller. The safety partner is a co-processor that provides redundancy for safety-related functions in the system.

The primary controller configures the safety partner. Only one download of the user program to the primary controller is required. The operating mode of the safety partner is controlled by the primary controller.

Chassis

The chassis provides the physical connections between modules and the 1756 GuardLogix system. Any failure, though unlikely, would be detected as a failure by one or more of the active components of the system. Therefore, the chassis is not relevant to the safety discussion.

GuardLogix-XT™ controllers must use a ControlLogix-XT chassis to achieve the extreme environment rating.

Power Supplies

No extra configuration or wiring is required for SIL 3 operation of the ControlLogix power supplies. Any failure would be detected as a failure by one or more of the active components of the GuardLogix system. Therefore, the power supply is not relevant to the safety discussion.

GuardLogix-XT controllers must use a ControlLogix-XT power supply to achieve the extreme environment rating.

CIP Safety Protocol

Safety-related communication between GuardLogix controllers takes place via produced and consumed safety tags. These safety tags use the CIP Safety protocol, which is designed to preserve data integrity during communication.

For more information on safety tags, see Chapter 5, Characteristics of Safety Tags, the Safety Task, and Safety Programs.

Safety I/O Devices

For information on CIP Safety I/O devices for use with GuardLogix controllers, see Chapter 3.

Communication Bridges

Table 5 lists the communication interface modules available to facilitate communication over EtherNet/IP, DeviceNet, and ControlNet networks via the CIP Safety protocol.

Table 5 - Communication Interface Modules by System

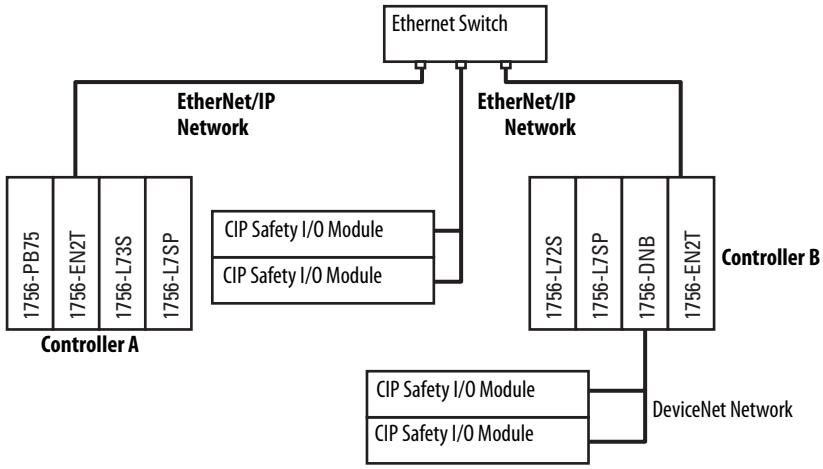
GuardLogix System	Communication Modules
1756	• 1756-ENBT, 1756-EN2T(R), 1756-EN2F, or 1756-EN3TR EtherNet/IP bridge • 1734-AENT POINT I/O Ethernet adapter • 1756-DNB DeviceNet bridge • 1756-CN2 ControlNet bridge • 1756-CN2R Redundant ControlNet bridge
1756 -XT	• 1756-EN2TXT, 1756-EN2TRXT EtherNet/IP bridge - XT (copper) • 1756-CN2RXT Redundant XT ControlNet bridge
1768	• 1768-ENBT • 1734-AENT POINT I/O Ethernet adapter • 1768-CNB • 1768-CNBR

IMPORTANT Due to the design of the CIP Safety control system, CIP Safety bridge devices, like the bridges listed in the table, are not required to be SIL 3-certified.

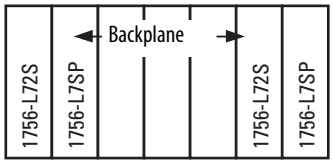
EtherNet/IP Network

Peer-to-peer safety communication between GuardLogix controllers is possible via the EtherNet/IP network through the use of EtherNet/IP bridges. An EtherNet/IP bridge lets the GuardLogix controller control and exchange safety data with CIP Safety I/O devices on an EtherNet/IP network.

Figure 4 - Peer-to-peer Communication via EtherNet/IP Bridges and the EtherNet/IP Network



TIP Peer-to-peer safety communication between two GuardLogix controllers in the same chassis is also possible via the backplane.

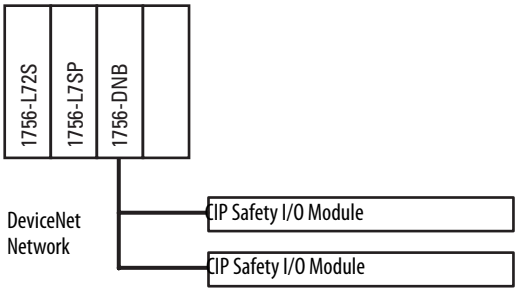


.

DeviceNet Safety Network

DeviceNet bridges let the GuardLogix controller control and exchange safety data with CIP Safety I/O modules on a DeviceNet network.

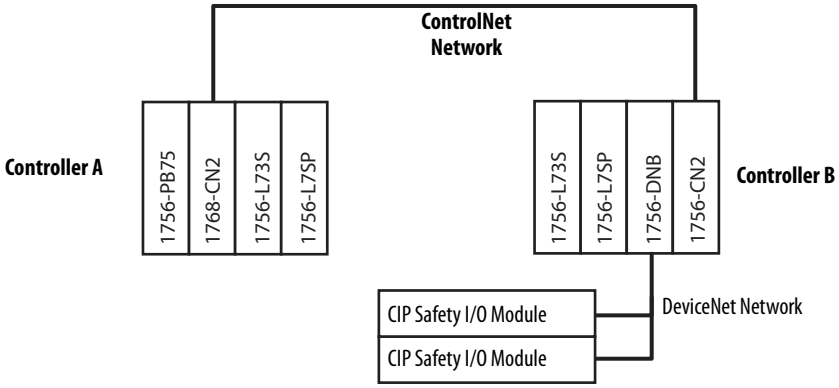
Figure 5 - Communication via a DeviceNet Bridge



ControlNet Network

ControlNet bridges let the GuardLogix controller produce and consume safety tags over ControlNet networks to other GuardLogix controllers or remote CIP Safety I/O networks.

Figure 6 - Communication via a ControlNet Bridge



Programming Overview

Program GuardLogix 5570 controllers by using the Studio 5000 Logix Designer application.

Use the Logix Designer application to define the location, ownership, and configuration of I/O devices and controllers and create, test, and debug program logic. Only relay ladder logic is supported in the GuardLogix safety task.

See Appendix A for information on the set of logic instructions available for safety projects.

Authorized personnel can change a safety program, but only by using one of the processes that are described in Editing Your Safety Application on page 59.

Notes:

CIP Safety I/O for the GuardLogix Control System

Overview

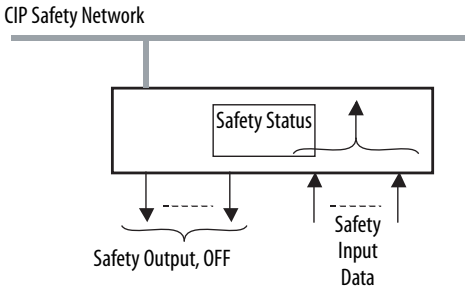
Before operating a GuardLogix 5570 safety system that contains CIP Safety I/O devices, you must read, understand, and follow the installation, operation, and safety information that is provided in the publications that are listed in the SIL 3-certified GuardLogix Components tables on page 16.

CIP Safety I/O devices can be connected to safety input and output devices, like sensors and actuators, that let these devices be monitored and controlled by the GuardLogix controller. For safety data, I/O communication is performed through safety connections by using the CIP Safety protocol; safety logic is processed in the GuardLogix controller.

Typical Safety Functions of CIP Safety I/O Devices

The following is treated as the safe state by CIP Safety I/O devices:

- Safety outputs: OFF
- Safety input data to controller: OFF



Use CIP Safety I/O devices for applications that are in the safe state when the safety output turns OFF.

Diagnostics

CIP Safety I/O devices perform self-diagnostics when the power is turned ON and periodically during operation. If a diagnostic failure is detected, safety input data (to the controller) and local safety outputs are set to their safe state (OFF).

Status Data

In addition to safety input and output data, CIP Safety I/O devices support status data to monitor device and I/O circuit health. See your device's product documentation for specific product capabilities.

Status Indicators

The CIP Safety I/O devices include status indicators. For details on status indicator operation, refer to the product documentation for your specific device.

On- or Off-delay Function

Some CIP Safety I/O devices can support On-delay and Off-delay functions for input signals. Depending upon your application, you may need to include Off-delay, On-delay, or both when you calculate system reaction time.

See Appendix C for information on system reaction time.

Reaction Time

The input reaction time is the time from when the signal changes on an input terminal to when safety data is sent to the GuardLogix controller.

The output reaction time is the time from when safety data is received from the GuardLogix controller to when the output terminal changes state.

For information on how to determine the input and output reaction times, refer to the product documentation for your specific CIP Safety I/O device.

See Appendix C for information on how to calculate the system reaction time.

Safety Considerations for CIP Safety I/O Devices

You must commission all devices with a node or IP address and communication rate, if necessary, before their installation on a safety network.

Ownership

Each CIP Safety I/O device in a GuardLogix system is owned by one GuardLogix controller. Multiple GuardLogix controllers and multiple CIP Safety I/O devices can be used without restrictions in chassis or on networks as needed. When a controller owns an I/O device, it stores the device's configuration data, as defined by the user. This configuration controls how the devices operate in the system.

From a control standpoint, safety output devices can be controlled by only one controller. Each safety input device is also owned by a single controller; however, safety input data can be shared (consumed) by multiple GuardLogix controllers.

Safety I/O Configuration Signature

The configuration signature defines the device's configuration. It can be read and monitored. The configuration signature is used to uniquely identify a device's configuration. When using a GuardLogix controller, you do not have to monitor this signature. The GuardLogix controller automatically monitors the signature.

Safety I/O Device Replacement

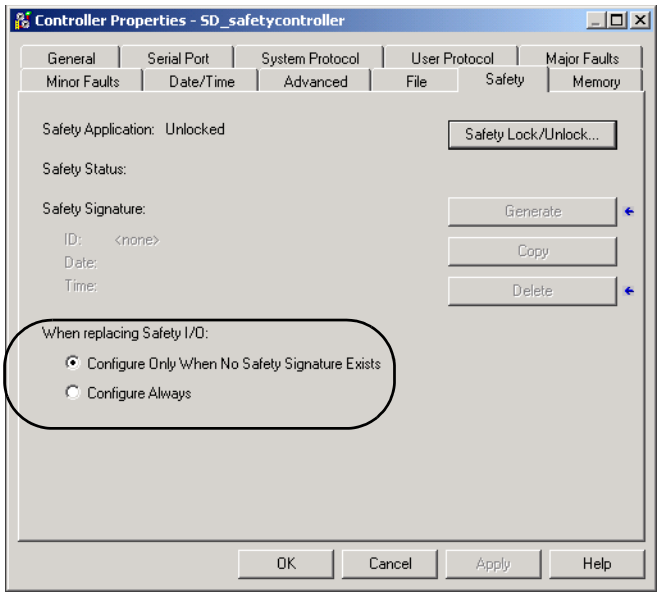
The replacement of safety devices requires that the replacement device be configured properly and that the replacement device's operation be user-verified.

ATTENTION: During replacement or functional testing of a device, the safety of the system must not rely on any portion of the affected device.

Two options for I/O device replacement are available on the Safety tab of the Controller Properties dialog box in the Logix Designer application:

- Configure Only When No Safety Signature Exists
- Configure Always

Figure 7 - Safety I/O Replacement Options



Configure Only When No Safety Signature Exists

This setting instructs the GuardLogix controller to configure a safety device only when the safety task does not have a safety task signature, and the replacement device is in an out-of-box condition, meaning that a safety network number does not exist in the safety device.

If the safety task has a safety task signature, the GuardLogix controller configures only the replacement CIP Safety I/O device if the following is true:

- The device already has the correct safety network number.
- The device electronic keying is correct.
- The node or IP address is correct.

Configure Always

The GuardLogix controller always attempts to configure a replacement CIP Safety I/O device if the device is in an out-of-box condition, meaning that a safety network number does not exist in the replacement safety device, and the node number and I/O device keying matches the controller's configuration.

ATTENTION: Enable the Configure Always feature only if the entire routable CIP Safety control system is not being relied on to maintain SIL 3 behavior during the replacement and functional testing of a device.

If other parts of the CIP Safety control system are being relied upon to maintain SIL 3, make sure that the controller's Configure Always feature is disabled.

It is your responsibility to implement a process to make sure proper safety functionality is maintained during device replacement.

ATTENTION: Do not place any devices in the out-of-box condition on any CIP Safety network when the Configure Always feature is enabled, except while following the device replacement procedure in the GuardLogix5570 Controllers User Manual, publication 1756-UM022.

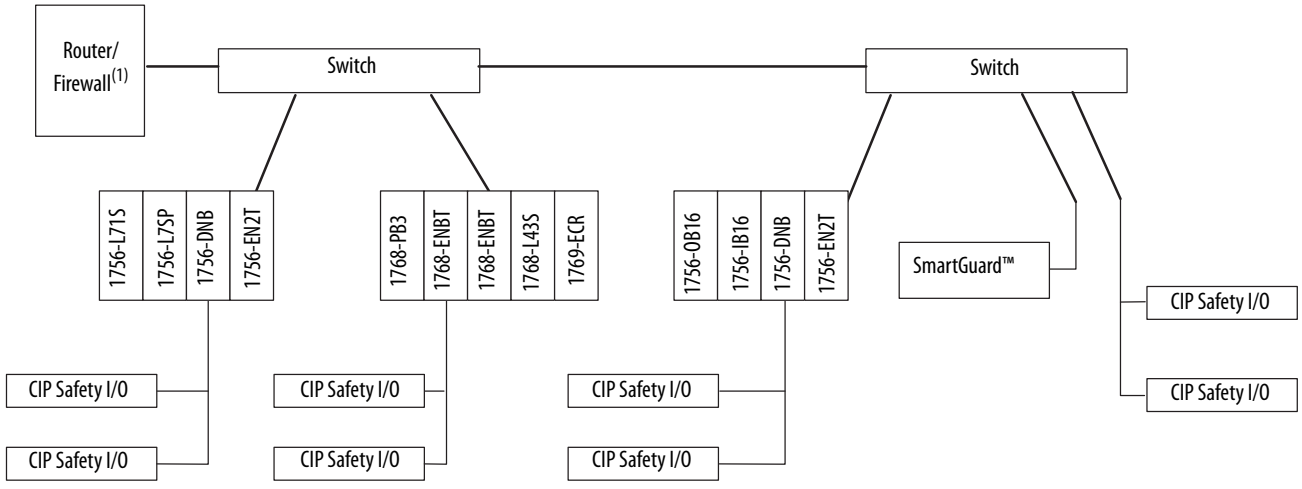
Notes:

CIP Safety and the Safety Network Number

Routable CIP Safety Control System

To understand the safety requirements of a CIP Safety control system, including the safety network number (SNN), you must first understand how communication is routable in CIP control systems. The CIP Safety control system represents a set of interconnected CIP Safety devices. The routable system represents the extent of potential mis-routing of packets from an originator to a target within the CIP Safety control system. The system is isolated such that there are no other connections into the system. For example, because the system in Figure 8 cannot be interconnected to another CIP Safety system through a larger, plant-wide ethernet backbone, it illustrates the extent of a routable CIP Safety system.

Figure 8 - CIP Safety System Example



(1) The router or firewall is configured to limit traffic.

Unique Node Reference

The CIP Safety protocol is an end-node to end-node safety protocol. The CIP Safety protocol allows the routing of CIP Safety messages to and from CIP Safety devices through non-certified bridges, switches, and routers.

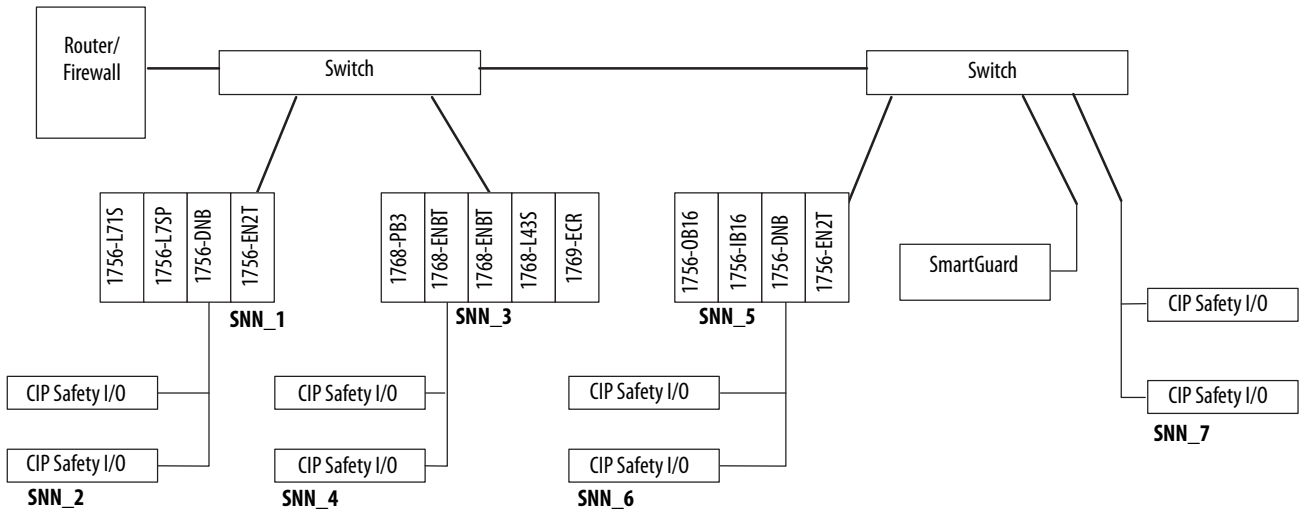
To prevent errors in non-certified bridges, switches, or routers from becoming dangerous, each end node within a routable CIP Safety control system must have a unique node reference. The unique node reference is a combination of a safety network number (SNN) and the node address of the node.

Safety Network Number

The safety network number (SNN) is assigned automatically by the software or manually by you. Each CIP Safety network that contains safety I/O nodes must have at least one unique SNN. Each chassis that contains one or more safety devices must have at least one unique SNN. Safety network numbers that are assigned to each safety network or network subnet must be unique.

TIP Multiple SNNs can be assigned to a CIP Safety subnet or a chassis that contains multiple safety devices. However, for simplicity, we recommend that each CIP Safety subnet have one, and only one, unique SNN. This recommendation also applies for each chassis.

Figure 9 - CIP Safety Example with More Than One SNN

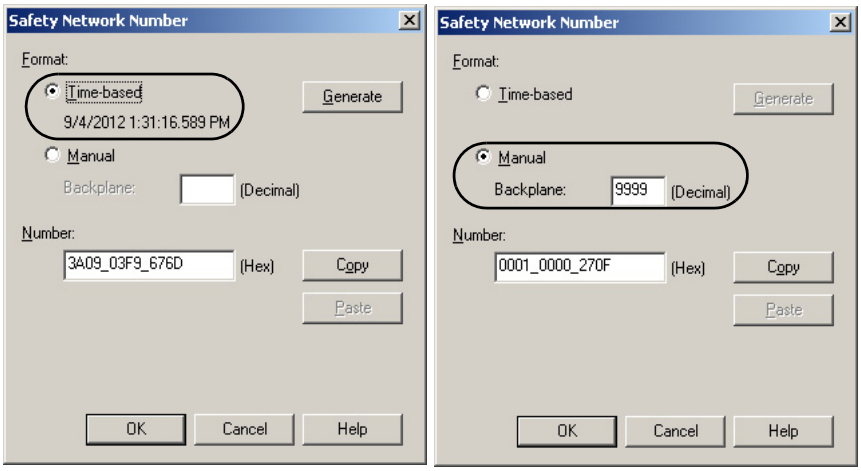


Each CIP Safety device must be configured with an SNN. Any device that originates a safety connection to another safety device must be configured with the SNN of the target device. If the CIP Safety system is in the start-up process before the functional safety testing of the system, the originating device can be used to set the unique node reference into the device.

The SNN used by the system is a 6-byte hexadecimal number. The SNN can be set and viewed in one of two formats: time-based or manual. When the

time-based format is selected, the SNN represents a localized date and time. When the manual format is selected, the SNN represents a network type and a decimal value from 1...9999.

Figure 10 - SNN Formats



The assignment of a time-based SNN is automatic when you create a GuardLogix safety controller project and add new CIP Safety I/O devices.

Manual manipulation of an SNN is required in the following situations:

- If safety consumed tags are used
- If the project consumes safety input data from a device whose configuration is owned by some other safety device
- If a safety project is copied to a different hardware installation within the same routable CIP Safety system

IMPORTANT	If you assign an SNN manually, take care to make sure that system expansion does not result in duplication of SNN and node address combinations. A verification error occurs if your project contains duplicate SNN and node address combinations.

Considerations for Assigning the Safety Network Number (SNN)

The assignment of the SNN is dependent upon factors including the configuration of the controller or CIP Safety I/O device.

Safety Network Number (SNN) for Safety Consumed Tags

When a safety controller that contains produced safety tags is added to the I/O Configuration tree, the SNN of the producing controller must be entered. The SNN can be copied from the producing controller's project and pasted into the new controller being added to the I/O Configuration tree.

See the GuardLogix 5570 Controllers User Manual, publication 1756-UM022, for information on how to copy and paste an SNN.

Safety Network Number (SNN) for Out-of-box Devices

Out-of-box CIP Safety I/O devices do not have an SNN. The SNN is set when a configuration is sent to the device by the GuardLogix controller that owns the device.

IMPORTANT	To add a CIP Safety I/O device to a configured GuardLogix system (the SNN is present in the GuardLogix controller), the replacement CIP Safety I/O device must have the correct SNN applied before it is added to the CIP Safety network.

Safety Network Number (SNN) for Safety Device with a Different Configuration Owner

When a CIP Safety I/O device is owned by a different GuardLogix controller (controller B), and then is added to another GuardLogix project (controller A project), the Logix Designer application assigns the SNN based on the current project. Because the current project (controller A project) is not the true configuration owner, you need to copy the original SNN (controller B project) into the configuration in controller A's project. This is easy to do with standard copy and paste commands. The result is that the CIP Safety I/O device produces data to two GuardLogix controllers at the same time. You can do copy and paste for a maximum of 16 controllers.

Refer to the GuardLogix 5570 Controllers User Manual, publication 1756-UM022, for information on how to change, copy, and paste safety network numbers.

Safety Network Number (SNN) When Copying a Safety Project

ATTENTION: If a safety project is copied for use in another project with different hardware or in a different physical location, and the new project is within the same routable CIP Safety system, every SNN must be changed in the second system. SNN values must not be repeated.

See the GuardLogix 5570 Controllers User Manual, publication 1756-UM022, for information on how to change the SNN.

Characteristics of Safety Tags, the Safety Task, and Safety Programs

Differentiate between Standard and Safety

Because it is a Logix-series controller, both standard (non-safety-related) and safety-related components can be used in the GuardLogix control system.

You can perform standard automation control from standard tasks within a GuardLogix project. GuardLogix controllers provide the same functionality as other ControlLogix series controllers. What differentiates GuardLogix controllers from standard controllers is that they provide a SIL 3-capable safety task.

However, a logical and visible distinction is required between the standard and safety-related portions of the application. The Logix Designer application provides this differentiation via the safety task, safety programs, safety routines, safety tags, and safety I/O devices. You can implement both SIL 2 and SIL 3 levels of safety control with the safety task of the GuardLogix controller.

SIL 2 Safety Applications

You can perform SIL 2 safety control by using the GuardLogix controller's safety task.

Because GuardLogix controllers are part of the ControlLogix series of processors, you can perform SIL 2 safety control with a GuardLogix controller by using standard tasks or the safety task. This capability provides unique and versatile safety-control options, as most applications have a higher percentage of SIL 2 safety functions than SIL 3 safety functions.

SIL 2 Safety Control in the Safety Task

The GuardLogix safety task can be used to provide SIL 2 and SIL 3 safety functions. If SIL 3 safety functions need to be performed simultaneously with SIL 2 safety functions, you must fulfill the requirements that are defined in the SIL 3 Safety–the Safety Task, Safety Programs, and Safety Routines sections of this chapter, as well as the SIL 2 requirements that are listed in this section.

SIL 2 Safety Logic

From a GuardLogix safety control perspective, the biggest difference between SIL 2 and SIL 3 safety-rated devices is that SIL 2 is generally single-channel, while SIL 3 is typically dual channel. When using Guard safety-rated I/O (red modules), which is required in the safety task, SIL 2 safety inputs can be single channel, which can reduce complexity and the number of modules that are necessary.

It is up to the safety system designer to implement all safety functions properly. Consideration must be given to the following:

- Field device selection (properly select, identify, and mitigate all device faults)
- Consider safety demand requirements (low IEC 61511 or high ISO 13849)
- Consider test intervals (diagnostics and proof testing that is needed to satisfy application requirements)
- Identify and justify with proper documentation any fault exclusions that are used

IMPORTANT	If a combination of SIL 2 and SIL 3 safety functions are used simultaneously within the safety task, you must prevent SIL 2 input signals from directly controlling SIL 3 safety functions. Use specific safety-task programs or routines to separate SIL 2 and SIL 3 safety functions.

Within the safety task, the Logix Designer application includes a set of safety-related ladder-logic instructions. GuardLogix controllers also feature application-specific SIL 3-rated safety instructions. All of these logic instructions can be used in CAT. 1...4 and SIL 1...3 safety functions.

For SIL 2-only safety, a safety task signature is not required. However, if any SIL 3 safety functions are used within the safety task, a safety task signature is required.

For SIL 2 applications, we recommend that you safety-lock the safety task once testing is completed. Locking the safety task enables more security features. You can also use FactoryTalk® Security and Logix Designer routine source protection to limit access to safety-related logic.

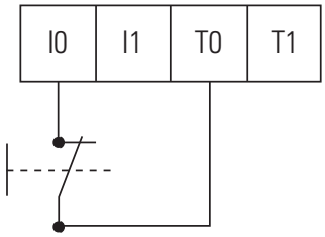
For more information on how to generate a safety task signature and safety-locking the safety task, refer to the GuardLogix 5570 Controllers User Manual, publication 1756-UM022.

SIL 2 Safety Inputs

CompactBlock™ Guard I/O™ (1791-series), ArmorBlock® Guard I/O (1732-series), and POINT Guard I/O (1734-series) safety input modules support single-channel SIL 2 safety input circuits. Because these modules are also rated for SIL 3 operation, mixing SIL 2 and SIL 3 circuits on the same module is allowed, provided you follow these guidelines.

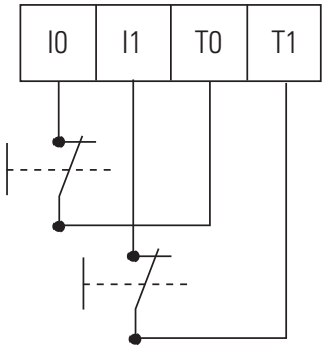
These two wiring examples show how to wire SIL 2 safety circuits to Guard I/O safety input modules. These examples use onboard test sources (T0...T*x*) that are resident on all 1791 and 1732 safety input modules.

Figure 11 - Input Wiring



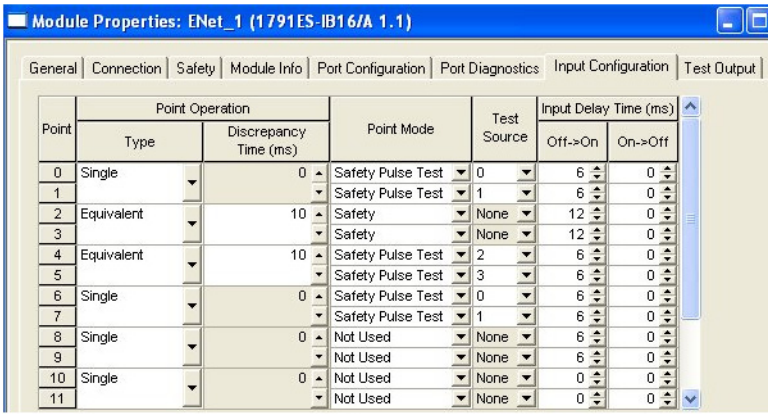
Guard I/O modules group inputs in pairs to facilitate Cat. 3, Cat. 4, and SIL 3 safety functions. For use in Cat. 1, Cat. 2, and SIL 2 safety functions, module inputs should still be used in pairs as illustrated. Two SIL 2 safety functions are shown wired to inputs I0 and I1 using test sources T0 and T1, respectively.

Figure 12 - Input Wiring in Pairs



For Cat. 1, Cat. 2, and SIL 2 safety functions, the Guard I/O safety modules need specific configurations within the GuardLogix project. In this example, inputs 0, 1, 6, 7, 8, 9, 10, and 11 are part of a Cat. 1, 2 or SIL 2 safety function. Inputs 2 and 3, as well as 4 and 5 are part of a Cat. 3, Cat. 4, or SIL 3 safety function.

Figure 13 - Input Configuration



Field	Value
Type	Single
Discrepancy Time	N/A
Point Mode	Safety Pulse Test
Test Source	Set values based on how the field device is physically wired to the module. To make sure the test source is properly enabled, open and view settings on the Test Output tab.
Input Delay Time	User input based on field device characteristics.

IMPORTANT The onboard pulse test outputs (T0…Tx) are typically used with field devices that have mechanical contacts. If a safety device that has electronic outputs is used (to feed safety inputs), they must have the appropriate safety ratings.

IMPORTANT If you are using GuardLogix Safety Application Instructions, be sure to configure your safety input modules as single, not equivalent or complementary. These instructions provide all dual-channel functionality necessary for PLd (Cat. 3) or PLe (Cat. 4) safety functions.

See the GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095.

SIL 2 Safety Control in Standard Tasks

Because of the quality and amount of diagnostics that are built into the ControlLogix series of controllers, you can perform SIL 2 safety functions from within standard tasks. This is also true for GuardLogix controllers.

To perform SIL 2 safety control within a GuardLogix standard task, you must abide by requirements that are defined in the Using ControlLogix in SIL 2 Applications Safety Reference Manual, publication 1756-RM001.

SIL 3 Safety–the Safety Task

Creation of a GuardLogix project automatically creates a single safety task. The safety task has these additional characteristics:

- GuardLogix controllers are the only controllers that support the safety task.
- The safety task cannot be deleted.
- GuardLogix controllers support a single safety task.
- Within the safety task, you can use multiple safety programs that are composed of multiple safety routines.
- You cannot schedule or execute standard routines from within the safety task.

The safety task is a periodic timed task with a user-selectable task priority and watchdog. In most cases, it is the controller's top priority and the user-defined program watchdog must be set to accommodate fluctuations in the execution of the safety task.

Safety Task Limitations

You specify both the safety task period and the safety task watchdog. The safety task period is the period at which the safety task executes. The safety task watchdog is the maximum time that is allowed from the start of safety task scheduled execution to its completion.

For more information on the safety task watchdog, see Appendix C, Reaction Times.

The safety task period is limited to a maximum of 500 ms and cannot be modified online. Make sure that the safety task has enough time to finish before it is triggered again. Safety-task watchdog timeout, a nonrecoverable safety fault in the GuardLogix controller, occurs if the safety task is triggered while it is still executing from the previous trigger.

See Chapter 7, Monitor Status and Handle Faults, for more information.

Safety Task Execution Details

The safety task executes in the same manner as standard periodic tasks, with the following exceptions:

- The safety task does not begin executing until the primary controller and safety partner have established their control partnership and the coordinated system time (CST) is synchronized. However, standard tasks begin executing as soon as the controller transitions to Run mode.
- Although the configurable range of the requested packet interval (RPI) for safety inputs and safety consumed tags is 6...500 ms, safety input tags and safety-consumed tags are updated only at the beginning of safety task execution. This means that even though the I/O RPI can be faster than the safety task period, the data does not change during safety task execution. The data is read only once at the beginning of the safety task execution.
- Safety input values are frozen at the start of safety task execution. As a result, timer-related instructions, such as TON and TOF, will not update during a single safety-task execution. They will keep accurate time from one task execution to another, but the accumulated time will not change during safety task execution.

ATTENTION: This behavior differs from standard Logix task execution, but is similar to PLC or SLC™ behavior.

- For standard tags that are mapped to safety tags, the standard tag values are copied into safety memory at the start of the safety task and do not change during safety task execution.
- Safety output tag (output and produced) values are updated at the conclusion of safety task execution.

- The safety task responds to mode changes (for example, Run to Program or Program to Run) at timed intervals. As a result, the safety task can take more than one task period, but always less than two, to make a mode transition.

IMPORTANT	While safety-unlocked and without a safety task signature, the controller prevents simultaneous write access to safety memory from the safety task and communication commands. As a result, the safety task can be held off until a communication update completes. The time that is required for the update varies by tag size. Therefore, safety connection and safety watchdog timeouts could occur. (For example, if you make online edits when the safety task rate is set to 1 ms, a safety watchdog timeout could occur.) To compensate for the hold-off time due to a communication update, add 2 ms to the safety watchdog time. When the controller is safety-locked or a safety task signature exists, the situation that is described in this note cannot occur.

Use of Human-to-machine Interfaces

Follow these precautions and guidelines for using HMI devices in SIL-rated GuardLogix systems.

Precautions

You must exercise precautions and implement specific techniques on HMI devices. These precautions include, but are not restricted to the following:

- Limited access and security
- Specifications, testing, and validation
- Restrictions on data and access
- Limits on data and parameters

For more information on how HMI devices fit into a typical SIL loop, see Figure 1 on page 15.

Use sound techniques in the application software within the HMI and controller.

Accessing Safety-related Systems

HMI- related functions consist of two primary activities: reading and writing data.

Reading Parameters in Safety-related Systems

Reading data is unrestricted because reading doesn't affect the behavior of the safety system. However, the number, frequency, and size of the data being read can affect controller availability. To avoid safety-related nuisance trips, use good communication practices to limit the impact of communication processing on the controller. Do not set read rates to the fastest rate possible.

Changing Parameters in SIL-rated Systems

A parameter change in a safety-related loop via an external (that is, outside the safety loop) device (for example, an HMI) is allowed only with the following restrictions:

- Only authorized, specially trained personnel (operators) can change the parameters in safety-related systems via HMIs.
- The operator who makes changes in a safety-related system via an HMI is responsible for the effect of those changes on the safety loop.
- You must clearly document variables that are to be changed.
- You must use a clear, comprehensive, and explicit operator procedure to make safety-related changes via an HMI.
- Changes can be accepted in a safety-related system only if the following sequence of events occurs:

  a. The new variable must be sent twice to two different tags; that is, both values must not be written to with one command.
  b. Safety-related code that executes in the controller, must check both tags for equivalency and make sure they are within range (boundary checks).
  c. Both new variables must be read back and displayed on the HMI device.
  d. Trained operators must visually check that both variables are the same and are the correct value.
  e. Trained operators must manually acknowledge that the values are correct on the HMI screen that sends a command to the safety logic, which allows the new values to be used in the safety function.

  In every case, the operator must confirm the validity of the change before they are accepted and applied in the safety loop.

- Test all changes as part of the safety validation procedure.

- Sufficiently document all safety-related changes that are made via the HMI, including the following:
  - Authorization
  - Impact analysis
  - Execution
  - Test information
  - Revision information
- Changes to the safety-related system must comply with IEC 61511 standard on process safety, section 11.7.1 Operator Interface requirements.
- Changes to the safety-related system must comply with IEC 62061 for machine safety.
- The developer must follow the same sound development techniques and procedures that are used for other application software development, including the verification and testing of the operator interface and its access to other parts of the program. In the controller application software, create a table that is accessible by the HMI and limit access to required data points only.
- Similar to the controller program, the HMI software needs to be secured and maintained for SIL-level compliance after the system has been validated and tested.

Safety Programs

A safety program has all of the attributes of a standard program, except that it can be scheduled only in the safety task. A safety program can also define program-scoped safety tags. A safety program can be scheduled or unscheduled.

A safety program can contain only safety components. All routines in a safety program are safety routines. A safety program cannot contain standard routines or standard tags.

Safety Routines

Safety routines have all of the attributes of standard routines, except that they can exist only in safety programs. One safety routine can be designated as the main routine. Another safety routine can be designated as the fault routine. Only safety-certified instructions may be used in safety routines.

For a listing of safety instructions, see Appendix A.

ATTENTION: To preserve SIL 3, you must make sure that your safety logic does not attempt to read or write standard tags.

Safety Tags

The GuardLogix control system supports the use of both standard and safety tags in the same project. However, the programming software operationally differentiates standard tags from safety tags.

Safety tags have all of the attributes of standard tags with the addition of mechanisms to provide SIL 3 data integrity.

Table 6 - Valid Data Types for Safety Tags

- AUX_VALVE_CONTROL
- BOOL
- CAM_PROFILE
- CAMSHAFT_MONITOR
- CB_CONTINUOUS_MODE
- CB_CRANKSHAFT_POS_MONITOR
- CB_INCH_MODE
- CB_SINGLE_STROKE_MODE
- CONFIGURABLE_ROUT
- CONNECTION_STATUS
- CONTROL
- COUNTER
- DCA_INPUT
- DCI_MONITOR
- DCI_START
- DCI_STOP
- DCI_STOP_TEST
- DCI_STOP_TEST_LOCK
- DCI_STOP_TEST_MUTE
- DINT
- DIVERSE_INPUT
- EIGHT_POS_MODE_SELECTOR
- EMERGENCY_STOP
- ENABLE_PENDANT
- EXT_ROUTINE_CONTROL
- EXT_ROUTINE_PARAMETERS
- FBD_BIT_FIELD_DISTRIBUTE
- FBD_CONVERT
- FBD_COUNTER
- FBD_LOGICAL
- FBD_MASK_EQUAL
- FBD_MASKED_MOVE
- FBD_TIMER
- FIVE_POS_MODE_SELECTOR
- INT
- LIGHT_CURTAIN
- MAIN_VALVE_CONTROL
- MANUAL_VALVE_CONTROL
- MUTING_FOUR_SENSOR_BIDIR
- MUTING_TWO_SENSOR_ASYM
- MUTING_TWO_SENSOR_SYM
- MOTION_INSTRUCTION
- PHASE
- PHASE_INSTRUCTION
- REAL
- REDUNDANT_INPUT
- REDUNDANT_OUTPUT
- SAFETY_MAT
- SERIAL_PORT_CONTROL
- SFC_ACTION
- SFC_STEP
- SFC_STOP
- SINT
- STRING
- THRS_ENHANCED
- TIMER
- TWO_HAND_RUN_STATION

The Logix Designer application prevents the direct creation of invalid tags in a safety program. If invalid tags are imported, they cannot be verified.

IMPORTANT	Aliasing between standard and safety tags is prohibited in safety applications.

Tags that are classified as safety tags are either controller-scoped or program-scoped. Controller-scoped safety tags can be read by either standard or safety logic or other communication devices, but can be written to only by safety logic or another GuardLogix safety controller. Program-scoped safety tags are accessible only by local safety routines. These are routines that reside within the safety program.

Tags that are associated with Safety I/O and produced or consumed safety data must be controller-scoped safety tags.

IMPORTANT	Any controller-scoped safety tag is readable by any standard routine, but the update rate is based on the execution of the safety task. Thus, safety tags are updated at the safety task periodic rate, which is different from standard tag behavior.

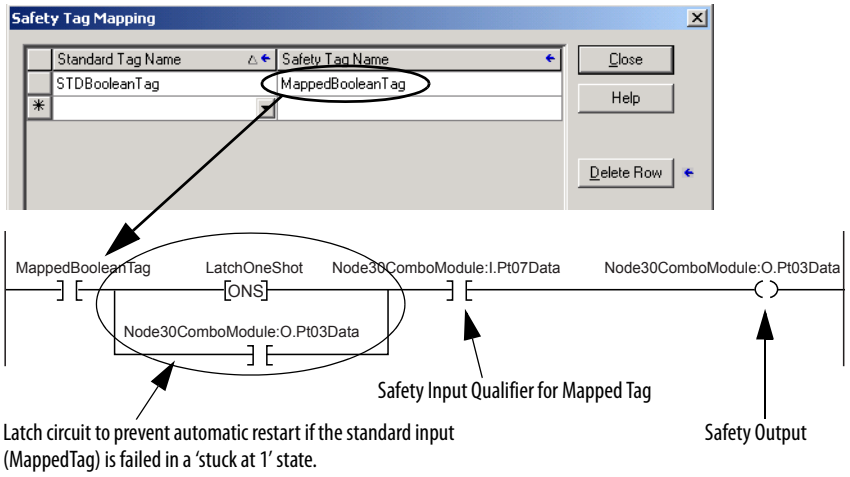
Standard Tags in Safety Routines (tag mapping)

Controller-scoped standard tags can be mapped into safety tags, providing you with a mechanism to synchronize standard and safety actions.

ATTENTION: When using standard data in a safety routine, you are responsible for providing a reliable means to make sure that the data is used in an appropriate manner. The use of standard data in a safety tag does not make it safety data. You must not directly control a safety output with standard tag data.

This example illustrates how to qualify the standard data with safety data.

Figure 14 - Qualify Standard Data with Safety Data



Notes:

Safety Application Development

Safety Concept Assumptions

The safety concept assumes the following:

- If you are responsible for creating, operating, and maintaining the application, you are fully qualified, specially trained, and experienced in safety systems.
- You apply the logic correctly, meaning that programming errors can be detected. Programming errors can be detected by strict adherence to specifications, programming and naming rules.
- You perform a critical analysis of the application and use all possible measures to detect a failure.
- You confirm all application downloads via a manual check of the safety task signature.
- You perform a complete functional test of the entire system before the operational startup of a safety-related system.

Table 7 - Controller Modes

Controller Mode	Safety Task Status	Safety[1] (up to and including)	Comments (A valid program has been downloaded to the controller.)
Program	Unlocked No signature		• I/O connections established • Safety Task logic is not being scanned.
Run	Unlocked No signature	(Development purposes only)	• Forcing allowed • Online editing allowed. • Safety memory is isolated, but is unprotected (read/write). • Safety Task logic is being scanned. Primary and partner controllers process logic, cross-compare logic outputs. Logic outputs are written to safety outputs.
Run	Locked No signature	PLd/Cat. 3 Control reliable SIL CL2	• New forces are not allowed. Existing forces are maintained. • Online editing is not allowed. • Safety memory is protected (read only). • Safety task logic is scanned. • Primary and partner controllers process logic, cross-compare logic outputs. Logic outputs are written to safety outputs.
Run	Unlocked With signature	Ple/Cat. 4 Control reliable SIL CL3	• Forces are not allowed. (They must be removed to generate a safety task signature.) • Online editing is not allowed. • Safety memory is protected (read only). • Safety task logic is scanned. • Primary and partner controllers process logic, cross-compare logic outputs. Logic outputs are written to safety outputs. • Safety task signature is unprotected and can be deleted by anyone who has access to the controller.
Run	Locked With signature	Ple/Cat. 4 Control reliable SIL CL3	• Forces are not allowed. (They must be removed to generate a safety task signature.) • Online editing is not allowed. • Safety memory is protected (read only). • Safety task logic is scanned. • Primary and partner controllers process logic, cross-compare logic outputs. Logic outputs are written to safety outputs. • Safety task signature is protected. Users must enter the unlock password to unlock the controller before they can delete the safety task signature.

(1) To achieved this level, you must adhere to the safety requirements defined in this publication.

Basics of Application Development and Testing

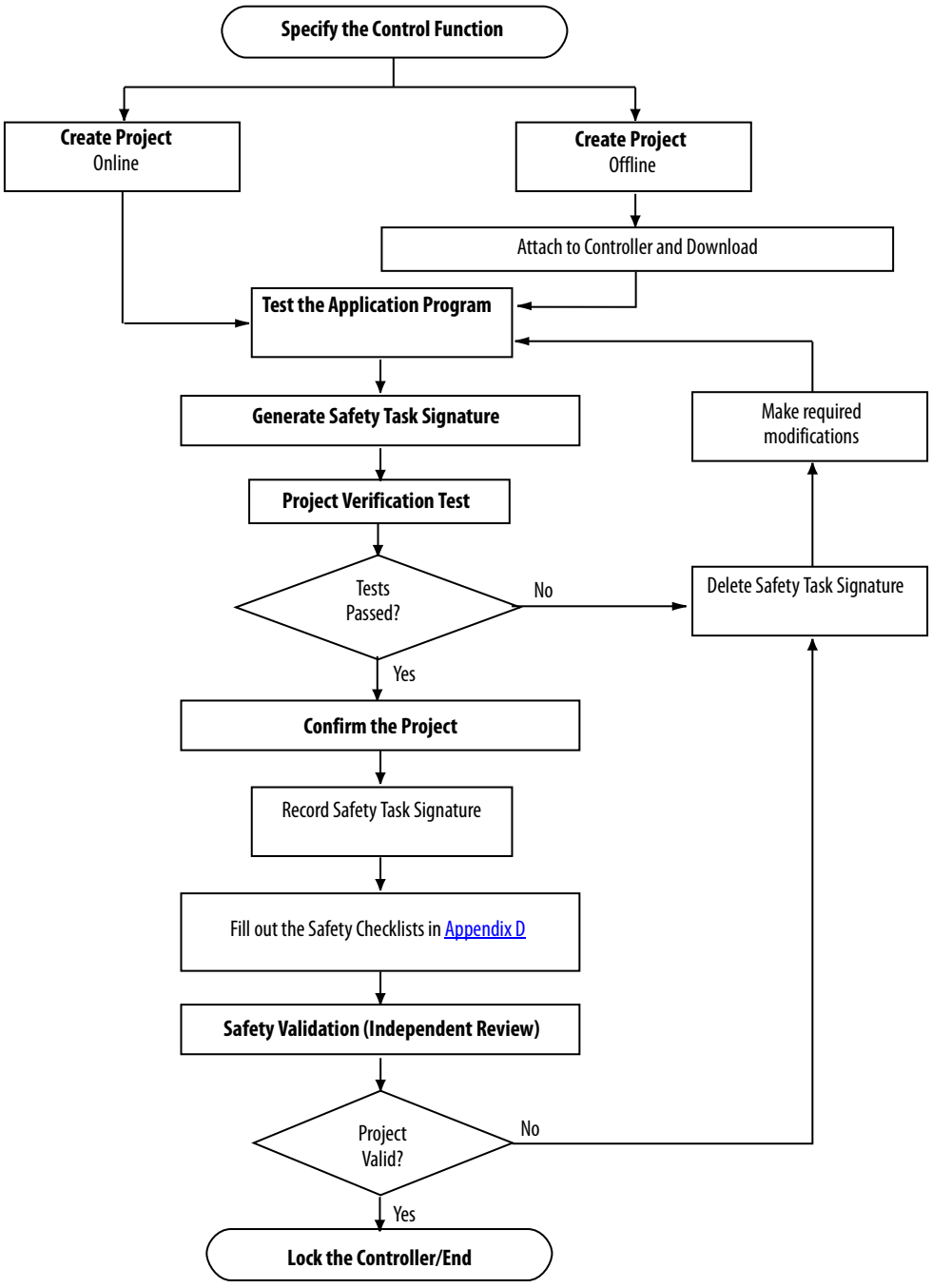
We recommend that the application program for the intended SIL CL3 system be developed by the system integrator or a user trained and experienced in safety applications. The developer must follow good design practices:

- Use functional specifications, including flow charts, timing diagrams, and sequence charts.
- Perform a review of safety task logic.
- Perform application validation.

Commissioning Life Cycle

The flowchart below shows the steps required for commissioning a GuardLogix system. The items in bold text are explained in the following sections.

Figure 15 - Commission the System



Specification of the Control Function

You must create a specification for your control function. Use this specification to verify that program logic correctly and fully addresses your application's functional and safety control requirements. The specification may be presented in a variety of formats, depending on your application. However, the specification must be a detailed description that includes the following (if applicable):

- Sequence of operations
- Flow and timing diagrams
- Sequence charts
- Program description
- Program print out
- Written descriptions of the steps with step conditions and actuators to be controlled, including the following:
  - Input definitions
  - Output definitions
  - I/O wiring diagrams and references
  - Theory of operation
- Matrix or table of stepped conditions and the actuators to be controlled, including the sequence and timing diagrams
- Definition of marginal conditions, for example, operating modes and EMERGENCY STOP

The I/O portion of the specification must contain the analysis of field circuits, that is, the type of sensors and actuators.

- Sensors (Digital or Analog)
  - Signal in standard operation (dormant current principle for digital sensors, sensors OFF means no signal)
  - Determination of redundancies required for SIL levels
  - Discrepancy monitoring and visualization, including your diagnostic logic
- Actuators
  - Position and activation in standard operation (normally OFF)
  - Safe reaction/positioning when switching OFF or power failure
  - Discrepancy monitoring and visualization, including your diagnostic logic

Create the Project

The logic and instructions used in programming the application must be the following:

- Easy to understand
- Easy to trace
- Easy to change
- Easy to test

Review and test all logic. Keep safety-related logic and standard logic separate.

Label the Program

The application program is clearly identified by one of the following:

- Name
- Date
- Revision
- Any other user identification

Test the Application Program

This step consists of any combination of Run and Program modes, online or offline edits, upload and download, and informal testing that is required to get an application running properly in preparation for the Project Verification test.

Generate the Safety Task Signature

The safety task signature uniquely identifies each project, including its logic, data, and configuration. The safety task signature is composed of an ID (identification number), date, and time.

You can generate the safety task signature if all of the following conditions are true:

- The Logix Designer application is online with the controller.
- The controller is in Program mode.
- The controller is safety-unlocked.
- The controller has no safety forces or pending online safety edits.
- The safety task status is OK.

Once application program testing is complete, you must generate the safety task signature. The programming software automatically uploads the safety task signature after it is generated.

IMPORTANT	To verify the integrity of every download, you must manually record the safety task signature after initial creation and check the safety task signature after every download to make sure that it matches the original.

You can delete the safety task signature only when the GuardLogix controller is safety-unlocked and, if online, the keyswitch is in the REM or PROG position.

When a safety task signature exists, the following actions are not permitted within the safety task:

- Online or offline programming or editing of safety components
- Forcing Safety I/O
- Data manipulation (except through routine logic or another GuardLogix controller)

Project Verification Test

To check your application program for adherence to the specification, you must generate a suitable set of test cases covering the application. The set of test cases must be filed and retained as the test specification.

You must include a set of tests to prove the validity of the calculations (formulas) used in your application logic. Equivalent range tests are acceptable. These are tests within the defined value ranges, at the limits, or in invalid value ranges. The necessary number of test cases depends on the formulas used and must comprise critical value pairs.

Active simulation with sources (field devices) must also be included, as it is the only way to verify that the sensors and actuators in the system are wired correctly. Verify the operation of programmed functions by manually manipulating sensors and actuators.

You must also include tests to verify the reaction to wiring faults and network communication faults.

Project verification includes tests of fault routines, and input and output channels, to be sure that the safety system operates properly.

To perform a project verification test on the GuardLogix controller, you must perform a full test of your application. You must toggle each sensor and actuator involved in every safety function. From a controller perspective, this means toggling the I/O point going into the controller, not necessarily the actual activators. Be sure to test all shutdown functions, because these functions are not typically exercised during normal operation. Also, be aware that a project verification test is valid only for the specific application tested. If the controller is moved to another application, you must also perform start-up and project

verification testing on the controller in the context of its new application program.

Confirm the Project

You must print or view the project, and compare the uploaded safety I/O and controller configurations, safety data, and safety task program logic to make sure that the correct safety components were downloaded, tested, and retained in the safety application program.

If your application program contains a safety Add-On Instruction that has been sealed with an instruction signature, you must also compare the instruction signature, date/time, and safety instruction signature to the values you recorded when you sealed the Add-On Instruction.

See Appendix B, Safety Add-On Instructions for information on creating and using safety Add-On Instructions in SIL 3 applications.

The steps below illustrate one method for confirming the project.

1. With the controller in Program mode, save the project.
2. Answer Yes to the Upload Tag Values prompt.
3. With the Logix Designer application offline, save the project with a new name, such as Offlineprojectname.ACD, where projectname is the name of your project.

   This is the new tested master project file.
4. Close the project.
5. Move the original project archive file out of its current directory. You can delete this file or store it in an archival location. This step is required because if the Logix Designer application finds the projectname.ACD in this directory, it will correlate it with the controller project and will not perform an actual upload.
6. With the controller still in Program mode, upload the project from the controller.
7. Save the uploaded project as Onlineprojectname.ACD, where projectname is the name of your project.
8. Answer Yes to the Upload Tag Values prompt.
9. Use the Logix Designer Program Compare utility to perform these comparisons:
   - Compare all of the properties of the GuardLogix controller and CIP Safety I/O devices.
   - Compare all of the properties of the safety task, safety programs and safety routines.
   - Compare all of the logic in the safety routines.

Safety Validation

An independent, third-party review of the safety system may be required before the system is approved for operation. An independent, third-party certification is required for IEC 61508 SIL 3.

Lock the GuardLogix Controller

The GuardLogix controller system can be safety-locked to help protect safety control components from modification. However, safety-locking the controller is not a requirement for SIL 3 applications. The safety-lock feature applies only to safety components, such as the safety task, safety programs, safety routines, safety tags, safety Add-On Instructions, safety I/O, and safety task signature. However, safety-locking alone does not satisfy SIL 3 requirements.

No aspect of safety can be modified while the controller is in the safety-locked state. When the controller is safety-locked, the following actions are not permitted in the safety task:

- Online or offline programming or editing
- Forcing safety I/O
- Data manipulation (except through routine logic or another GuardLogix controller)
- Creating or editing safety Add-On Instructions
- Generating or deleting the safety task signature

The default state of the controller is safety-unlocked. You may place the safety application in a safety-locked state regardless of whether you are online or offline, and regardless of whether you have the original source of the program. However, no safety forces or pending safety edits may be present. Safety-locked or -unlocked status cannot be modified when the keyswitch is in the RUN position.

To provide an additional layer of protection, separate passwords may be used for safety-locking or -unlocking the controller. Passwords are optional.

Downloading the Safety Application Program

Upon download, application testing is required unless a safety task signature exists.

IMPORTANT	To verify the integrity of every download, you must manually record the safety task signature after initial creation and check the safety task signature after every download to make sure that it matches the original.

Downloads to a safety-locked GuardLogix controller are allowed only if the safety task signature, the hardware series, and the operating system version of the

offline project all match those contained in the target GuardLogix controller and the controller's safety task status is OK.

IMPORTANT	If the safety task signature does not match and the controller is safety-locked, you must unlock the controller to download. In this case, downloading to the controller deletes the safety task signature. As a result, you must revalidate the application.

ATTENTION: The USB port is intended for temporary local programming purposes only and not intended for permanent connection.

Uploading the Safety Application Program

If the GuardLogix controller contains a safety task signature, the safety task signature will be uploaded with the project. This means that any changes to offline safety data will be overwritten as a result of the upload.

Online Editing

If there is no safety task signature and the controller is safety-unlocked, you can perform online edits to your safety routines.

TIP	You cannot edit standard or safety Add-On Instructions while online.

Pending edits cannot exist when the controller is safety-locked or when there is a safety task signature. Online edits may exist when the controller is safety-locked. However, they may not be assembled or cancelled.

TIP	Online edits in standard routines are unaffected by the safety-locked or -unlocked state.

See page 59 for more information on making edits to your application program.

Storing and Loading a Project from Nonvolatile Memory

GuardLogix 5570 controllers support firmware upgrades and user program storage and retrieval by using a memory card. In a GuardLogix system, only the primary controller uses a memory card for nonvolatile memory.

When you store a safety project on a memory card, Rockwell Automation recommends you select Remote Program as the Load mode, that is, the mode the controller enters following the load. Prior to actual machine operation, operator intervention is required to start the machine.

You can initiate a load from nonvolatile memory only under these conditions:

- If the controller type specified by the project stored in nonvolatile memory matches your controller type
- If the major and minor revisions of the project in nonvolatile memory matches the major and minor revisions of your controller
- If your controller is not in Run mode

Loading a project to a safety-locked controller is allowed only when the safety task signature of the project stored in nonvolatile memory matches the project on the controller. If the signatures do not match or the controller is safety-locked without a safety task signature, you must first unlock the controller before attempting to update the controller via nonvolatile memory.

IMPORTANT	If you unlock the controller and initiate a load from nonvolatile memory, the safety-lock status, passwords, and safety task signature will be set to the values contained in nonvolatile memory once the load is complete.

Force Data

All data contained in an I/O, produced, or consumed safety tag, including CONNECTION_STATUS, can be forced while the project is safety-unlocked and no safety task signature exists. However, forces must be uninstalled, not just disabled, on all safety tags before the safety project can be safety-locked or a safety task signature can be generated. You cannot force safety tags while the project is safety-locked or when a safety task signature exists.

TIP	You can install and uninstall forces on standard tags regardless of the safety-locked or -unlocked state.

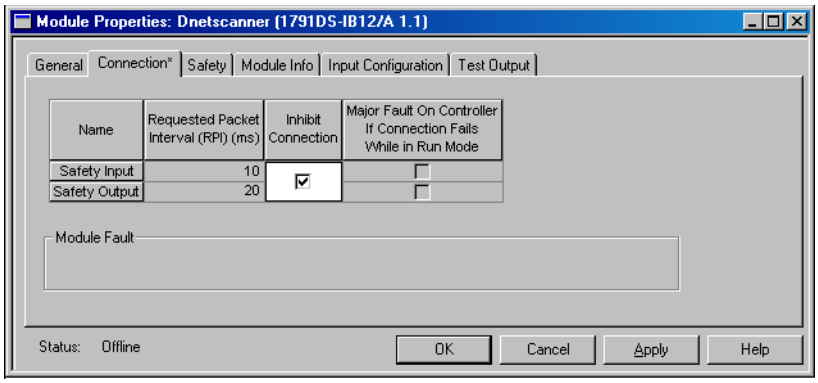
Inhibit a Device

You cannot inhibit or uninhibit CIP Safety I/O devices or producer controllers if the application program is safety-locked or a safety task signature exists.

Follow these steps to inhibit a specific safety I/O device.

1. In the Logix Designer application, right-click the device and choose Properties.
2. On the Module Properties dialog box, click the Connection tab.

3. Check Inhibit Connection and click Apply.



The device is inhibited whenever the check box is checked. If a communication device is inhibited, all downstream devices are also inhibited.

Editing Your Safety Application

The following rules apply to changing your safety application program in the Logix Designer application:

- Only authorized, specially-trained personnel can make program edits. These personnel should use all supervisory methods available, for example, using the controller keyswitch and software password protections.
- When authorized, specially-trained personnel make program edits, they assume the central safety responsibility while the changes are in progress. These personnel must also maintain safe application operation.
- When editing online, you must use an alternate protection mechanism to maintain the safety of the system.
- You must sufficiently document all program edits, including the following:
  - Authorization
  - Impact analysis
  - Execution
  - Test information
  - Revision information
- If online edits exist only in the standard routines, those edits are not required to be validated before returning to normal operation.
- You must make sure that changes to the standard routine, with respect to timing and tag mapping, are acceptable to your safety application.
- You **can** edit the logic portion of your program while offline or online, as described in the following sections.

Performing Offline Edits

When offline edits are made to only standard program elements, and the safety task signature matches following a download, you can resume operation.

When offline edits affect the safety program, you must revalidate all affected elements of the application, as determined by the impact analysis, before resuming operation.

The flowchart on page 61 illustrates the process for offline editing.

Performing Online Edits

If online edits affect the safety program, you must revalidate all affected elements of the application, as determined by the impact analysis, before resuming operation. The flowchart on page 61 illustrates the process for online editing.

TIP Limit online edits to minor program modifications such as setpoint changes or minor logic additions, deletions, and modifications.

Online edits are affected by the safety-lock and safety task signature features of the GuardLogix controller.

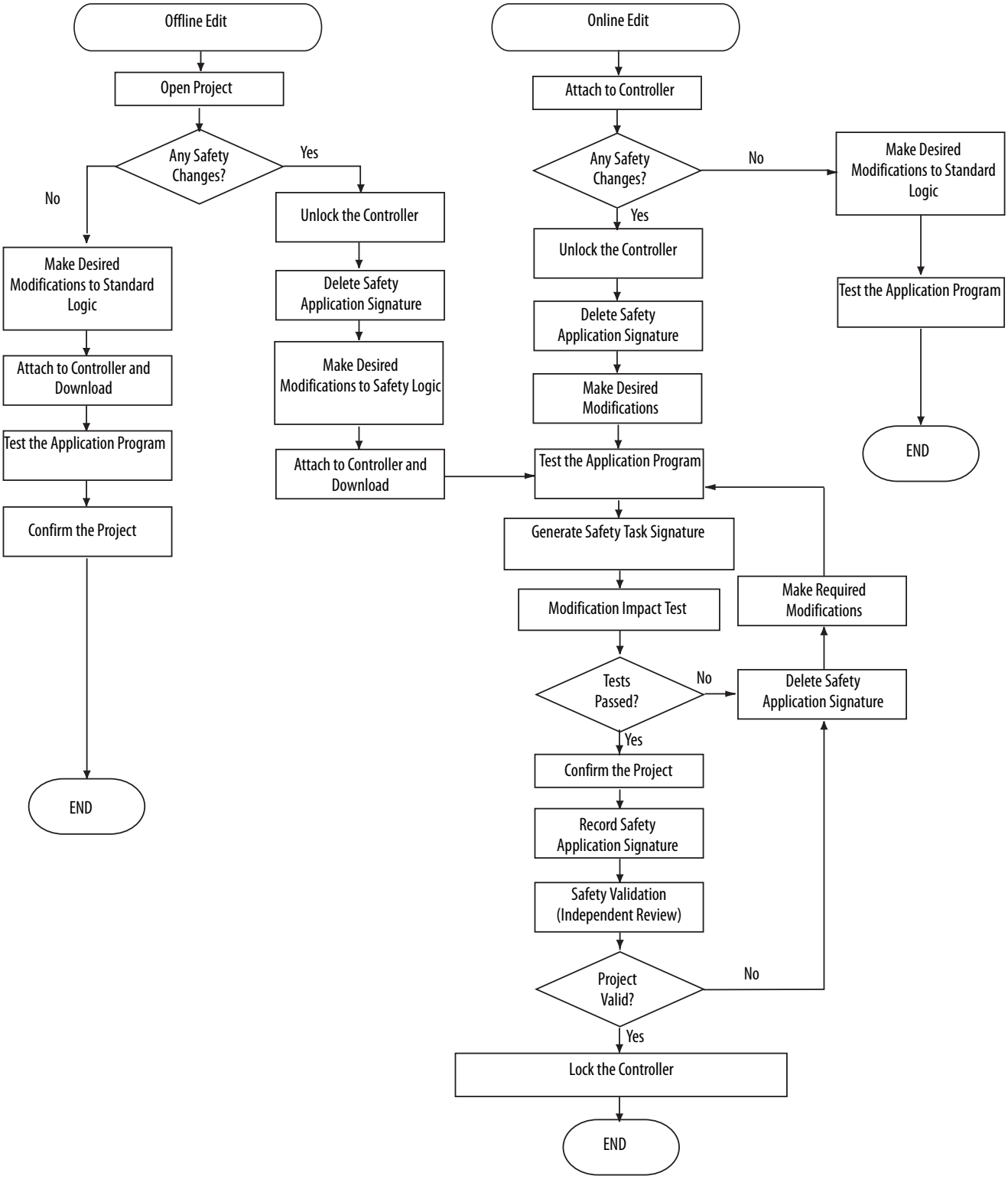
See Generate the Safety Task Signature on page 53 and Lock the GuardLogix Controller on page 56 for more information.

For detailed information on how to edit ladder logic in the Logix Designer application while online, see the Logix5000 Controllers Quick Start, publication 1756-QS001.

Modification Impact Test

Any modification, enhancement, or adaptation of your validated software must be planned and analyzed for any impact to the functional safety system. All appropriate phases of the software safety lifecycle need to be carried out as indicated by the impact analysis. At a minimum, functional testing of all impacted software must be carried out. All modifications to your software specifications must be documented. Test results must also be documented. Refer to IEC 61508-3, Section 7.8 Software Modification, for detailed information.

Figure 16 - Online and Offline Edit Process



Notes:

Monitor Status and Handle Faults

The GuardLogix architecture provides you with many ways of detecting and reacting to faults in the system. The first way that you can handle faults is to make sure you have completed the checklists for your application (see Appendix D).

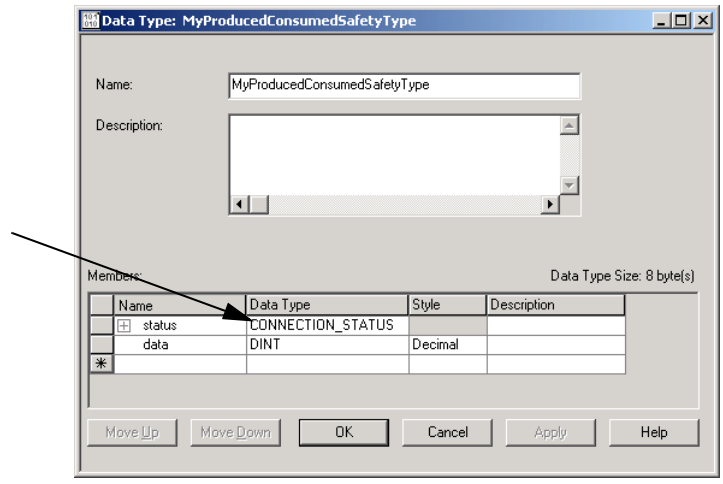
Monitoring System Status

You can view the status of safety tag connections. You can also determine current operating status by interrogating various device objects. It is your responsibility to determine what data is most appropriate to initiate a shutdown sequence.

CONNECTION_STATUS Data

The first member of the tag structure associated with safety input data and produced/consumed safety tag data contains the status of the connection. This member is a pre-defined data type called CONNECTION_STATUS.

Figure 17 - Data Type Dialog Box



The first two bits of the CONNECTION_STATUS data type contain a device's RunMode and ConnectionFaulted status bits. The following table describes the combinations of the RunMode and ConnectionFaulted states.

Table 8 - Safety Connection Status

RunMode Status	ConnectionFaulted Status	Safety Connection Operation
1 = Run	0 = Valid	Data is actively being controlled by the producing device. The producing device is in Run mode.
0 = Idle	0 = Valid	The connection is active and the producing device is in the Idle state. The safety data is reset to zero.
0 = Idle	1 = Faulted	The safety connection is faulted. The state of the producing device is unknown. The safety data is reset to zero.
1	1	Invalid state.

ATTENTION: Safety I/O connections and produced/consumed connections cannot be automatically configured to fault the controller if a connection is lost and the system transitions to the safe state. Therefore, if you need to detect a device fault to be sure that the system maintains SIL 3, you must monitor the Safety I/O CONNECTION_STATUS bits and initiate the fault via program logic.

Input and Output Diagnostics

Guard I/O modules provide pulse test and monitoring capabilities. If the module detects a failure, it sets the offending input or output to its safety state and reports the failure to the controller. The failure indication is made via input or output status and is maintained for a configurable amount of time after the failure is repaired.

IMPORTANT You are responsible for providing application logic to latch these I/O failures and to make sure the system restarts properly.

I/O Device Connection Status

The CIP Safety protocol provides status for each I/O device in the safety system. If an input connection failure is detected, the operating system sets all device inputs to their de-energized (safety) state, and the associated input status to faulted. If an output connection failure is detected, the operating system sets the associated output status to faulted. The output device de-energizes the outputs.

IMPORTANT You are responsible for providing application logic to latch these I/O failures and to make sure the system restarts properly.

De-energize to Trip System

GuardLogix controllers are part of a de-energize to trip system, which means that zero is the safe state. Some, but not all, safety I/O device faults cause all device inputs or outputs to be set to zero (safe state). Faults associated to a specific input channel result in that specific channel being set to zero; for example, a pulse test fault that is specific to channel 0 results in channel 0 input data being set to the safe state (0). If a fault is general to the device and not to a specific channel, the combined status bit displays the fault status and all device data is set to the safe state (0).

For information on how to use GuardLogix safety application instructions, see Appendix F of this manual and the GuardLogix Safety Application Instructions Safety Reference Manual, publication 1756-RM095.

Get System Value (GSV) and Set System Value (SSV) Instructions

The GSV and SSV instructions let you get (GSV) and set (SSV) controller system data stored in device objects. When you enter a GSV/SSV instruction, the programming software displays the valid object classes, object names, and attribute names for each instruction. Restrictions exist for using the GSV and SSV instructions with safety components.

IMPORTANT	The safety task cannot perform GSV or SSV operations on standard attributes. The attributes of safety objects that can be written by the standard task are for diagnostic purposes only. They do not affect safety task execution.

For more information on which safety attributes are accessible via GSV and SSV instructions, refer to the GuardLogix 5570 Controllers User Manual, publication 1756-UM022.

For general information on using GSV and SSV instructions, refer to the Logix5000 Controllers General Instructions Reference Manual, publication 1756-RM003.

GuardLogix System Faults

Faults in the GuardLogix system fall into these three categories:

- Nonrecoverable controller faults
- Nonrecoverable safety faults
- Recoverable faults

For information on handling faults, refer to the GuardLogix 5570 Controllers User Manual, publication 1756-UM022.

Nonrecoverable Controller Faults

A nonrecoverable controller fault occurs if the controller's internal diagnostics fail. Partnership is lost when a nonrecoverable controller fault occurs in either the primary controller or the safety partner, causing the other to generate a nonrecoverable watchdog timeout fault. Standard task and safety task execution stops, and Safety I/O transitions to the safe state.

Recovery from a nonrecoverable controller fault requires a download of the application program.

Nonrecoverable Safety Faults

In the event of a non-recoverable safety fault, the controller logs the fault to the controller-scoped fault handler and shuts down the safety task, including Safety I/O and safety logic.

To recover from a nonrecoverable safety fault, safety memory is reinitialized either from the safety task signature (happens automatically when you clear the fault) or, if no safety task signature exists, via an explicit download of the safety project.

You can override the safety fault by clearing the fault log entry through the controller-scoped safety fault handler. This allows standard tasks to keep running.

ATTENTION: Overriding the safety fault does not clear it. If you override the safety fault, it is your responsibility to prove that doing so maintains SIL 3.

Recoverable Faults

Controller faults caused by user programming errors in a safety program trigger the controller to process the logic contained in the project's safety program fault handler. The safety program fault handler provides the application with the opportunity to resolve the fault condition and then recover.

ATTENTION: You must provide proof to your certifying agency that automatic recovery from recoverable faults maintains SIL 3.

When a safety program fault handler does not exist or the fault is not recovered by it, the controller processes the logic in the controller-scoped fault handler, terminating safety program logic execution and leaving safety I/O connections active, but idle.

IMPORTANT When the execution of safety program logic is terminated due to a recoverable fault that is not handled by the safety program fault handler, the safety I/O connections are closed and reopened to reinitialize safety connections.

If user logic is terminated as a result of a recoverable fault that is not recovered, safety outputs are placed in the safe state and the producer of safety-consumed tags commands the consumers to place them in a safe state.

TIP When using safety I/O for standard applications, safety I/O will be commanded to the safe state if user logic is terminated as a result of a recoverable fault that is not recovered.

If a recoverable safety fault is overridden in the controller-scoped fault handler, only standard tasks keep running. If the fault is not overridden, the standard tasks are also shut down.

ATTENTION: Overriding the safety fault does not clear it. If you override the safety fault, it is your responsibility to prove that doing so maintains SIL 3.

Notes:

Safety Instructions

For the latest information, see our safety certificates at http://www.rockwellautomation.com/products/certification/safety/.

Table 9 and Table 10 list the safety application instructions that are certified for use in SIL 3 applications.

Table 9 - General Safety-Application Instructions

Mnemonic	Name	Purpose	Certification
CROUT	Configurable Redundant Output	Controls and monitors redundant outputs.	• BG • TÜV
DCA	Dual Channel Input - Analog (integer version)	Monitors two analog values for deviation and range tolerance.	TÜV
DCAF	Dual Channel Input - Analog (floating point version)		
DCS	Dual Channel Input - Stop	Monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch.	• BG • TÜV
DCST	Dual Channel Input - Stop With Test	Monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch. It includes the added capability to initiate a functional test of the stop device.	• BG • TÜV
DCSTL	Dual Channel Input - Stop With Test and Lock	Monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch. It includes the added capability to initiate a functional test of the stop device. It can monitor a feedback signal from a safety device and issue a lock request to a safety device.	• BG • TÜV
DCSTM	Dual Channel Input - Stop With Test and Mute	Monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch. It includes the added capability to initiate a functional test of the stop device and the ability to mute the safety device.	TÜV
DCM	Dual Channel Input - Monitor	Monitors dual-input safety devices.	• BG • TÜV
DCSRT	Dual Channel Input - Start	Energizes dual-input safety devices whose main function is to start a machine safely, for example an enable pendant.	• BG • TÜV
SMAT	Safety Mat	Indicates whether the safety mat is occupied.	TÜV
THRSe	Two-Hand Run Station – Enhanced	Monitors two diverse safety inputs, one from a right-hand push button and one from a left-hand push button, to control a single output. Features configurable channel-to-channel discrepancy time and enhanced capability for bypassing a two-hand run station.	• BG • TÜV
TSAM	Two Sensor Asymmetrical Muting	Automatically disables the protective function of a light curtain temporarily, by using two muting sensors that are arranged asymmetrically.	TÜV
TSSM	Two Sensor Symmetrical Muting	Automatically disables the protective function of a light curtain temporarily, by using two muting sensors that are arranged symmetrically.	TÜV
FSBM	Four Sensor Bidirectional Muting	Automatically disables the protective function of a light curtain temporarily, by using four sensors that are arranged sequentially before and after the sensing field of the light curtain.	TÜV

Table 10 - Metal-Form Safety-Application Instructions

Mnemonic	Name	Purpose	Certification
CBCM	Clutch Brake Continuous Mode	Used for press applications where continuous operation is desired.	• BG • TÜV
CBIM	Clutch Brake Inch Mode	Used for press applications where minor slide adjustments are required, such as press setup.	• BG • TÜV
CBSSM	Clutch Brake Single Stoke Mode	Used in single-cycle press applications.	• BG • TÜV
CPM	Crankshaft Position Monitor	Used to determine the slide position of the press.	• BG • TÜV
CSM	Camshaft Monitor	Monitors motion for the start, stop, and run operations of a camshaft.	• BG • TÜV
EPMS	Eight-position Mode Selector	Monitors eight safety inputs to control one of the eight outputs that correspond to the active input.	• BG • TÜV
AVC	Auxiliary Valve Control	Controls an auxiliary valve that is used with a main valve.	TÜV
MVC	Main Valve Control	Controls and monitors a main valve.	• BG • TÜV
MMVC	Maintenance Manual Valve Control	Used to manually drive a valve during maintenance operations.	• BG • TÜV

Routines in the safety task can use these ladder-logic safety instructions.

Table 11 - Ladder Logic Safety Instructions

Type	Mnemonic	Name	Purpose
Array (File)	FAL(1)	File Arithmetic and Logic	Perform copy, arithmetic, logic, and function operations on data that is stored in an array
	FLL(1)	File Fill	Fill the element of an array with the Source Value, while leaving the source value unchanged
	FSC(1)	File Search and Compare	Compare the value in an array, element by element
	SIZE(1)	Size In Elements	Find the size of a dimension of an array
Bit	XIC	Examine If Closed	Enable outputs when a bit is set
	XIO	Examine If Open	Enable outputs when a bit is cleared
	OTE	Output Energize	Set a bit
	OTL	Output Latch	Set a bit (retentive)
	OTU	Output Unlatch	Clear bit (retentive)
	ONS	One Shot	Triggers an event to occur one time
	OSR	One Shot Rising	Triggers an event to occur one time on the false-to-true (rising) edge of change-of-state
	OSF	One Shot Falling	Triggers an event to occur one time on the true-to-false (falling) edge of change-of-state
Timer	TON	Timer On Delay	Time how long a timer is enabled
	TOF	Timer Off Delay	Time how long a timer is disabled
	RTO	Retentive Timer On	Accumulate time
	CTU	Count Up	Count up
	CTD	Count Down	Count down
	RES	Reset	Reset a timer or counter

Table 11 - Ladder Logic Safety Instructions

Type	Mnemonic	Name	Purpose
Compare	CMP[1][2]	Compare	Perform a comparison on the arithmetic operations you specify in the expression
	EQU	Equal To	Test whether two values are equal
	GEQ	Greater Than Or Equal To	Test whether one value is greater than or equal to a second value
	GRT	Greater Than	Test whether one value is greater than a second value
	LEQ	Less Than Or Equal To	Test whether one value is less than or equal to a second value
	LES	Less Than	Test whether one value is less than a second value
	MEQ	Masked Comparison for Equal	Pass source and compare values through a mask and test whether they are equal
	NEQ	Not Equal To	Test whether one value is not equal to a second value
	LIM	Limit Test	Test whether a value falls within a specified range
Move	CLR	Clear	Clear a value
	COP[3]	Copy	Copy a value
	MOV	Move	Copy a value
	MVM	Masked Move	Copy a specific part of an integer
	SWPB[1]	Swap Byte	Rearrange the bytes of a value
Logical	AND	Bitwise AND	Perform bitwise AND operation
	NOT	Bitwise NOT	Perform bitwise NOT operation
	OR	Bitwise OR	Perform bitwise OR operation
	XOR	Bitwise Exclusive OR	Perform bitwise exclusive OR operation
Program Control	JMP	Jump To Label	Jump over a section of logic that does not always need to be executed (skips to referenced label instruction)
	LBL	Label	Labels an instruction so that it can be referenced by a JMP instruction
	JSR	Jump to Subroutine	Jump to a separate routine
	RET	Return	Return the results of a subroutine
	SBR	Subroutine	Pass data to a subroutine
	TND	Temporary End	Mark a temporary end that halts routine execution
	MCR	Master Control Reset	Disable every rung in a section of logic
	AFI	Always False Instruction	Disable a rung
	NOP	No Operation	Insert a placeholder in the logic
	EVENT	Trigger Event Task	Trigger one execution of an event task[5]
Math/ Compute	ADD	Add	Add two values
	CPT[1]	Compute	Perform the arithmetic operation that is defined in the expression
	SUB	Subtract	Subtract two values
	MUL	Multiply	Multiply two values
	DIV	Divide	Divide two values
	MOD	Modulo	Determine the remainder after one value is divided by a second value
	SQR	Square Root	Calculate the square root of a value
	NEG	Negate	Take the opposite sign of a value
	ABS	Absolute Value	Take the absolute value of a value
I/O	GSV[4]	Get System Value	Get controller status information
	SSV[4]	Set System Value	Set controller status information

(1) Supported only on 1756-L7*x*S and 1756-L7*x*SXT controllers. For the data type REAL, a floating point format is supported for safety routines on 1756-L7*x*S and 1756-L7*x*SXT controllers.
(2) Advanced operands like SIN, COS, and TAN are not supported in safety routines.
(3) The length operand must be a constant when the COP instruction is used in a safety routine. The length of the source and the destination must be the same.
(4) See the GuardLogix 5570 Controllers User Manual, publication 1756-UM022, for special considerations when using the GSV and SSV instructions.
(5) The event instruction triggers a scan of the standard task.

IMPORTANT If you are using Motion Direct Commands with a Kinetix 5500 or K5700 servo drive or a PowerFlex 527 drive, see the following publications for information on how to use this feature in safety applications.

- Kinetix 5500 Servo Drives User Manual, publication 2198-UM001
- Kinetix 5700 Servo Drives User Manual, publication 2198-UM002
- PowerFlex 527 Adjustable Frequency AC Drive User Manual, publication 520-UM002

See these publications for more information.

Table 12 - Additional Resources

Resource	Description
GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Provides more information on the safety application instructions
Logix5000 Controllers General Instructions Reference Manual, publication 1756-RM003	Contains detailed information on the Logix instruction set

Safety Add-On Instructions

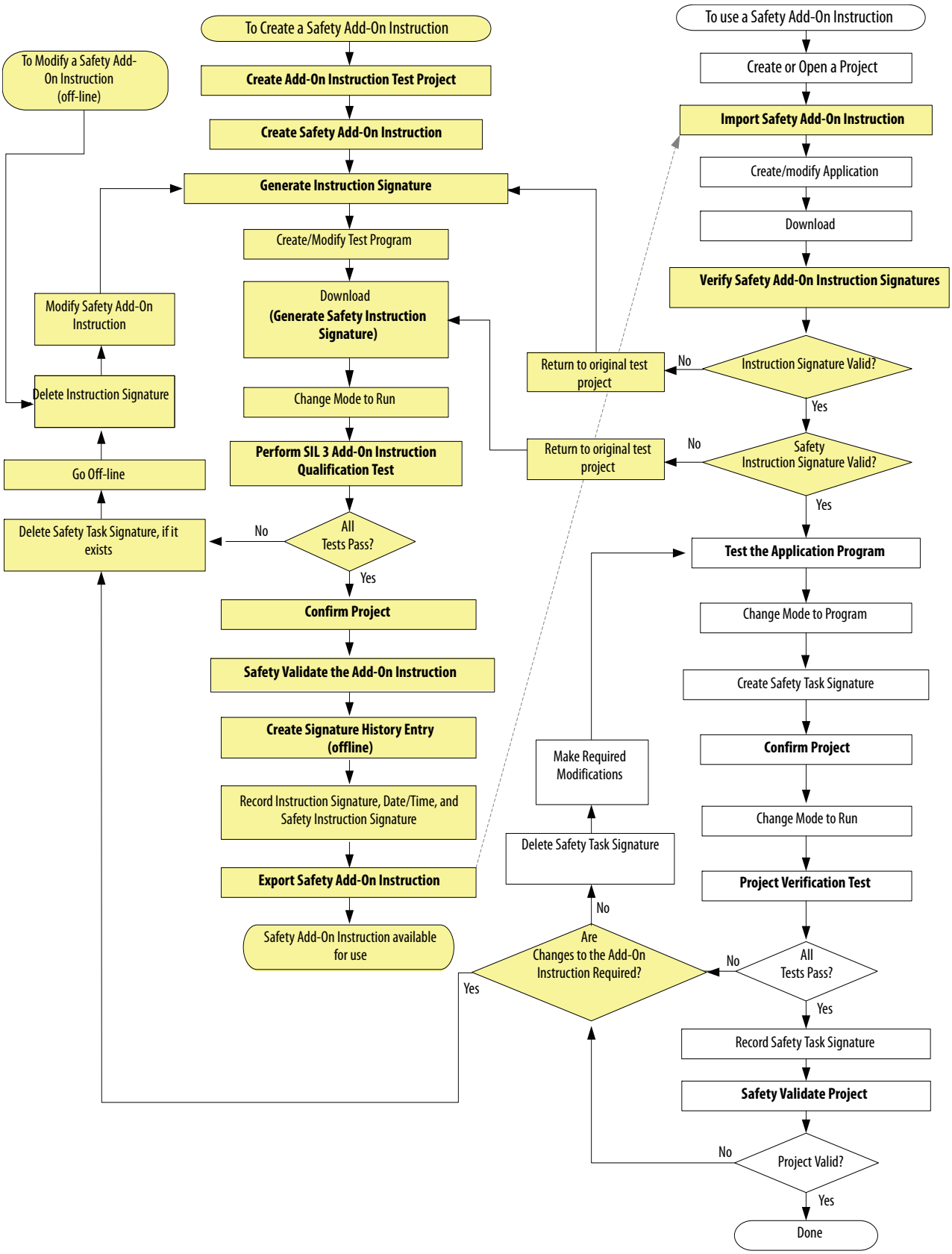
With the Logix Designer application, you can create safety Add-On Instructions. Safety Add-On Instructions let you encapsulate commonly used safety logic into a single instruction, which makes it modular and easier to reuse.

Safety Add-On Instructions use the instruction signature of high-integrity Add-On Instructions and also a SIL 3 safety instruction signature for use in safety-related functions up to and including SIL 3.

Create and Use a Safety Add-On Instruction

The flowchart on page 74 shows the steps that are required to create a safety Add-On Instruction and then use that instruction in a SIL 3 safety application program. The shaded items are steps unique to Add-On Instructions. The items in bold text are explained in the pages following the flowchart.

Figure 18 - Flowchart for Creating and Using Safety Add-On Instructions



Create Add-On Instruction Test Project

You must create a unique test project, specifically to create and test the safety Add-On Instruction. This project must be a separate and dedicated project to minimize any unexpected influences.

Follow the guidelines for projects that are described in Create the Project on page 53.

Create a Safety Add-On Instruction

For guidance in how to create Add-On Instructions, refer to the Logix5000 Controllers Add-On Instruction Programming Manual, publication 1756-PM010.

Generate Instruction Signature

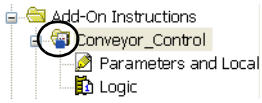
The instruction signature lets you quickly determine if the instruction has been modified. Each Add-On Instruction can have its own signature. The instruction signature is required when an Add-On Instruction is used in safety-related functions, and can sometimes be required for regulated industries. Use it when your application calls for a higher level of integrity.

The instruction signature consists of an ID number and time stamp that identifies the contents of the Add-On Instruction at a given point in time.

Once generated, the instruction signature seals the Add-On Instruction, which prevents it from being edited while the signature is in place. This restriction includes rung comments, tag descriptions, and any instruction documentation that was created. When the instruction is sealed, you can perform only these actions:

- Copy the instruction signature
- Create or copy a signature history entry
- Create instances of the Add-On Instruction
- Download the instruction
- Remove the instruction signature
- Print reports

When an instruction signature has been generated, the Logix Designer application displays the instruction definition with the seal icon.



IMPORTANT	If you plan to protect your Add-On Instruction by using the source protection feature in the Logix Designer application, you must enable source protection before you generate the instruction signature.

Download and Generate Safety Instruction Signature

When a sealed safety Add-On Instruction is downloaded for the first time, a SIL 3 safety instruction signature is automatically generated. The safety instruction signature is an ID number that identifies the execution characteristics of the safety Add-On Instruction.

SIL 3 Add-On Instruction Qualification Test

Safety Add-On Instruction SIL 3 tests must be performed in a separate, dedicated application to make sure unintended influences are minimized. You must follow a well-designed test plan and perform a unit test of the safety Add-On Instruction that exercises all possible execution paths through the logic, including the valid and invalid ranges of all input parameters.

Development of all safety Add-On Instructions must meet IEC 61508 - 'Requirements for software module testing', which provides detailed requirements for unit testing.

Confirm the Project

You must print or view the project, and manually compare the uploaded safety I/O and controller configurations, safety data, safety Add-On Instruction definitions, and safety-task program logic to make sure that the correct safety components were downloaded, tested, and retained in the safety application program.

See Confirm the Project on page 55 for a description of one method for confirming a project.

Safety Validate Add-On Instructions

An independent, third-party review of the safety Add-On Instruction may be required before the instruction is approved for use. An independent, third-party validation is required for IEC 61508 SIL 3.

Create Signature History Entry

The signature history provides a record for future reference. A signature history entry consists of the instruction signature, the name of the user, the time stamp value, and a user-defined description. Up to six history entries can be stored. You must be offline to create a signature history entry.

TIP The Signature Listing report in the Logix Designer application prints the instruction signature, the time stamp, and the safety instruction signature. To print the report, right-click Add-On Instruction in the Controller Organizer and choose Print>Signature Listing.

Export and Import the Safety Add-On Instruction

When you export a safety Add-On Instruction, choose the option to include all referenced Add-On Instructions and User-Defined Types in the same export file. By including referenced Add-On Instructions, you make it easier to preserve the signatures.

When importing Add-On Instructions, consider these guidelines:

- You cannot import a safety Add-On Instruction into a standard project.
- You cannot import a safety Add-On Instruction into a safety project that has been safety-locked or one that has a safety task signature.
- You cannot import a safety Add-On Instruction while online.
- If you import an Add-On Instruction with an instruction signature into a project where referenced Add-On Instructions or User-Defined Types are not available, you may need to remove the signature.

Verify Safety Add-On Instruction Signatures

After you download the application project that contains the imported safety Add-On Instruction, you must compare the instruction signature value, the date and time stamp, and the safety instruction signature values with the original values you recorded before you exported the safety Add-On Instruction. If they match, the safety Add-On Instruction is valid and you can continue with the validation of your application.

Test the Application Program

This step consists of any combination of Run and Program mode, online or offline program edits, upload and download, and informal testing that is required to get an application to run properly.

Project Verification Test

Perform an engineering test of the application, including the safety system.

See Project Verification Test on page 54 for more information on requirements.

Safety Validate Project

An independent, third-party review of the safety system may be required before the system is approved for operation. An independent, third-party validation is required for IEC 61508 SIL 3.

Additional Resources

For more information on how to use Add-On Instructions, refer to these publications.

Resource	Description
Logix5000 Controllers Add-On Instructions Programming Manual, publication 1756-PM010	Provides information on how to plan, create, use, import, and export Add-On Instructions in RSLogix 5000 applications
Import/Export Project Components Programming Manual, publication 1756-PM019	Contains detailed information on how to import and export project components

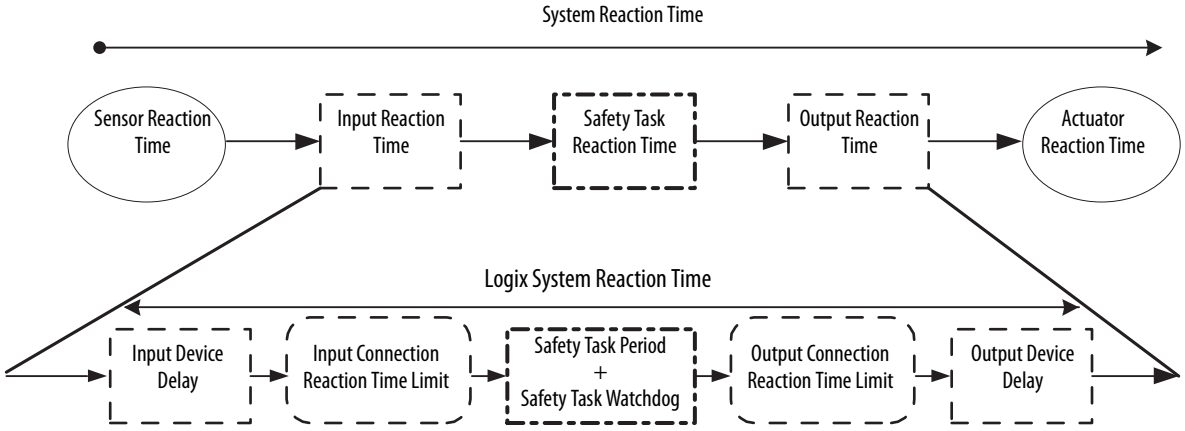
Reaction Times

System Reaction Time

To determine the system reaction time of any control chain, you must add up the reaction times of all of components of the safety chain.

System Reaction Time = Sensor Reaction Time + Logix System Reaction Time + Actuator Reaction Time

Figure 19 - System Reaction Time

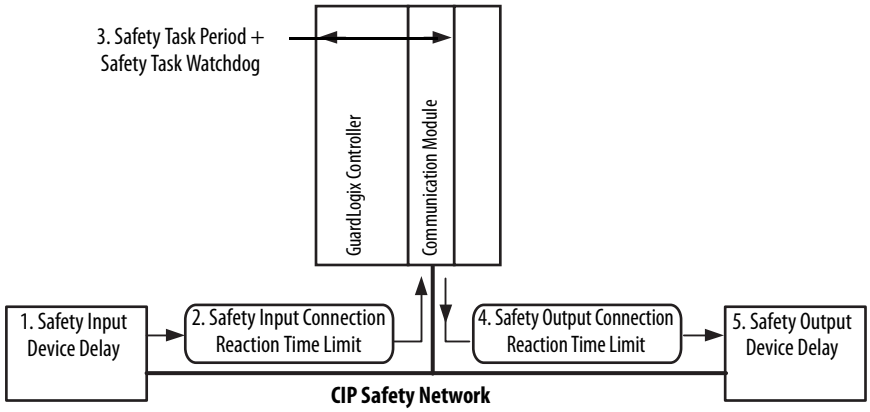


Logix System Reaction Time

The following sections provide information on how to calculate the Logix System Reaction Time for a simple input-logic-output chain and for a more complex application by using produced/consumed safety tags in the logic chain.

Simple Input-logic-output Chain

Figure 20 - Logix System Worst-case Reaction Time for Simple Input to Logic to Output



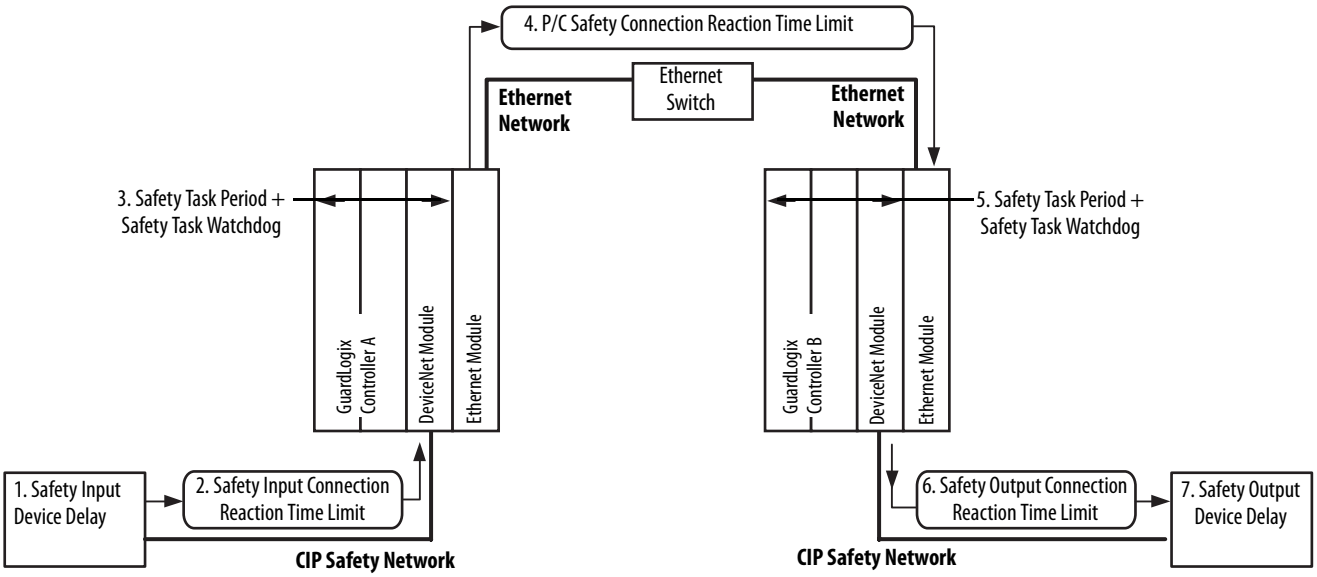
The Logix System Reaction Time for any simple input to logic to output chain consists of these five components:

1. Safety input device reaction time (plus input delay time, if applicable)
2. Safety Input Connection Reaction Time Limit
   (Read from the Module Properties dialog box in the Logix Designer application, this value is a multiple of the safety input device connection RPI.)
3. Safety Task Period plus Safety Task Watchdog time
4. Safety Output Connection Reaction Time Limit
   (Read from the Module Properties dialog box in the Logix Designer application, this value is a multiple of the safety task period.)
5. Safety output device reaction time

To aid you in determining the reaction time of your particular control loop, a Microsoft Excel spreadsheet is available in the Tools folder of the Studio 5000 environment DVD.

Logic Chain Using Produced/Consumed Safety Tags

Figure 21 - Logix System Reaction Time for Input to Controller A Logic to Controller B Logic to Output Chain



The Logix System Reaction Time for any input to controller A logic to controller B logic to output chain consists of these seven components:

1. Safety input device reaction time (plus input delay time, if applicable)
2. Safety Input Connection Reaction Time Limit
3. Safety Task Period plus Safety Task Watchdog time for Controller A
4. Produced/Consumed Safety Connection Reaction Time Limit
5. Safety Task Period plus Safety Task Watchdog time for Controller B
6. Safety Output Connection Reaction Time Limit
7. Safety output device reaction time

To aid you in determining the reaction time of your particular control loop, a Microsoft Excel spreadsheet is available in the Tools folder of the Studio 5000 environment DVD.

Factors Affecting Logix Reaction-time Components

The Logix Reaction Time components that are described in the previous sections can be influenced by a number of factors.

Table 13 - Factors Affecting Logix System Reaction-time

These Reaction Time Components	Are Influenced by the Following Factors
Input device delay	Input device reaction time
	On-Off and Off-On delay settings for each input channel, if applicable
Safety Input Connection Reaction Time Limit	Input device settings for: • Requested Packet Interval (RPI) • Timeout Multiplier • Delay Multiplier
	The amount of network communication traffic
	The EMC environment of the system
Safety Task Period and Safety Task Watchdog	Safety Task Period setting
	Safety Task Watchdog setting
	The number and execution time of instructions in the safety task
	Any higher priority tasks that may pre-empt safety task execution
Produced/Consumed Safety Connection Reaction Time Limit	Consumed tag settings for: • RPI • Timeout Multiplier • Delay Multiplier
	The amount of network communication traffic
	The EMC environment of the system
Output Connection Reaction Time Limit	Safety Task Period setting
	Output device's settings for: • Timeout Multiplier • Delay Multiplier
	The amount of network communication traffic
	The EMC environment of the system
Output module delay	Output module reaction time

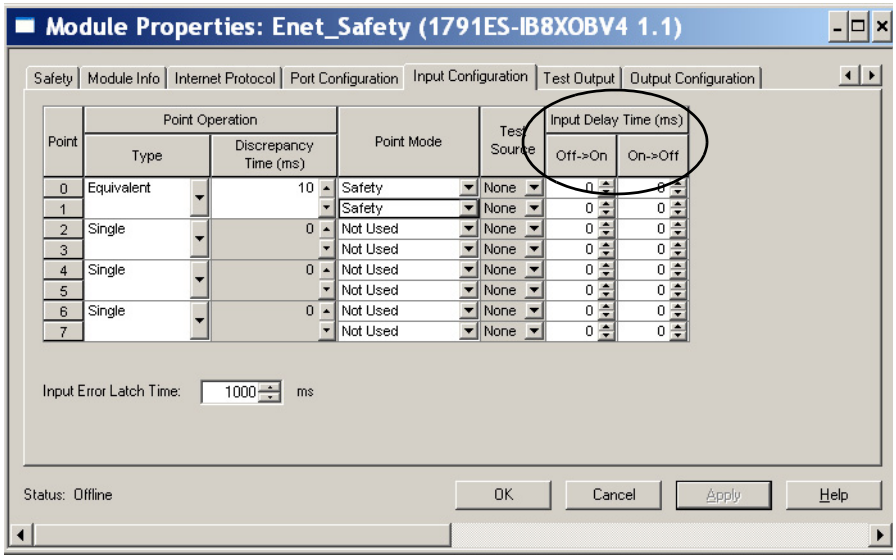
The following sections describe how to access data or settings for many of these factors.

Accessing Guard I/O Input Module Delay Time Settings

To configure input module delay time in the Logix Designer application, follow these steps.

1. In the configuration tree, right-click your Guard I/O module and choose Properties.
2. Click the Input Configuration tab.

3. Adjust the input delay time as required for your application.



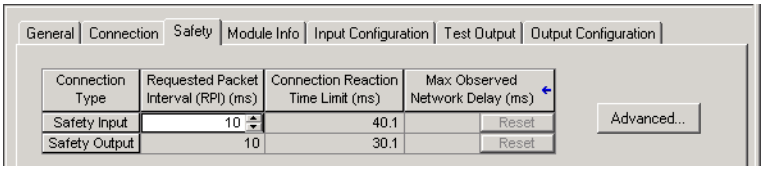
Access Input and Output Safety Connection Reaction Time Limit

The Connection Reaction Time Limit is defined by these three values:

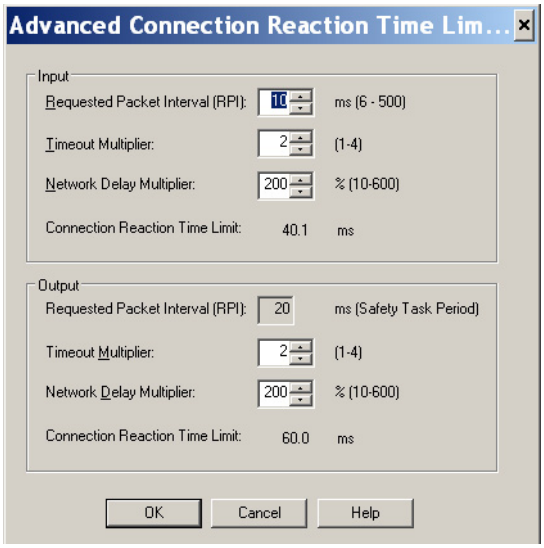
Value	Description
Requested Packet Interval (RPI)	How often the input and output packets are placed on the wire (network).
Timeout Multiplier	The Timeout Multiplier is essentially the number of retries before timing out.
Network Delay Multiplier	The Network Delay Multiplier accounts for any known delays on the wire. When these delays occur, timeouts can be avoided using this parameter.

By adjusting these values, you can adjust the Connection Reaction Time Limit. To view or configure these settings, follow these steps.

1. In the configuration tree, right-click your safety I/O device and choose Properties.
2. Click the Safety tab.



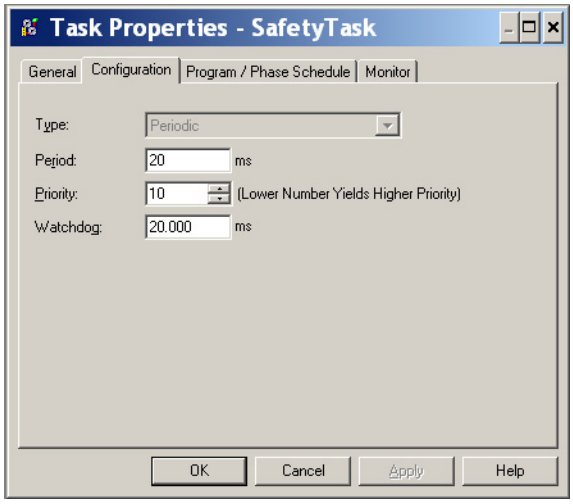
3. Click Advanced to open the Advanced Connection Reaction Time Limit dialog box.



Configuring the Safety Task Period and Watchdog

The safety task is a periodic timed task. You select the task priority and watchdog time via the Task Properties - Safety Task dialog box in your Logix Designer project.

To access the safety task period and watchdog time settings, right-click the Safety Task and choose Properties.

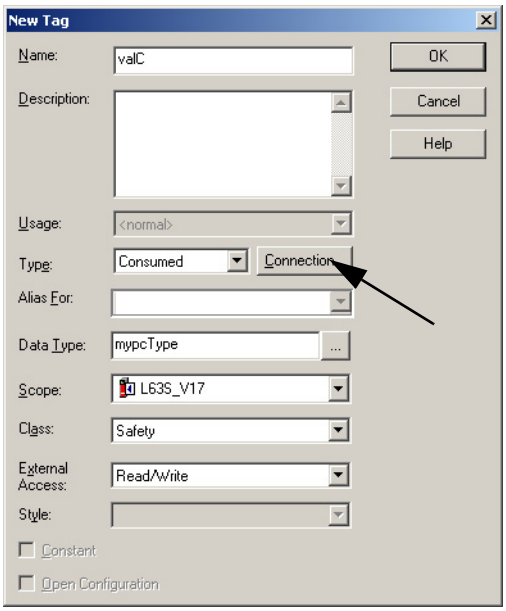


The priority of the safety task is not a safety concern, as the safety task watchdog monitors if the task is interrupted by higher priority task.

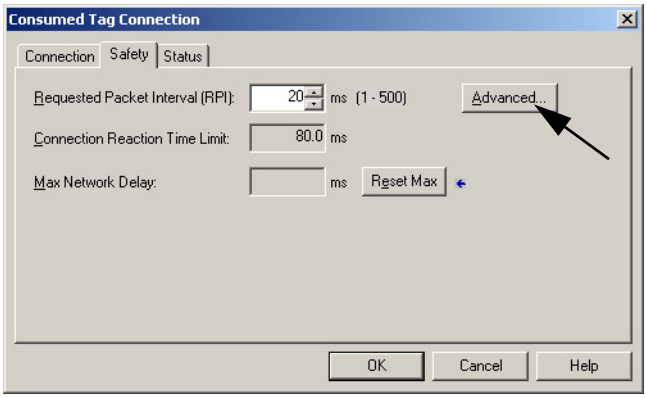
Accessing Produced/Consumed Tag Data

To view or configure safety-tag connection data, follow these steps.

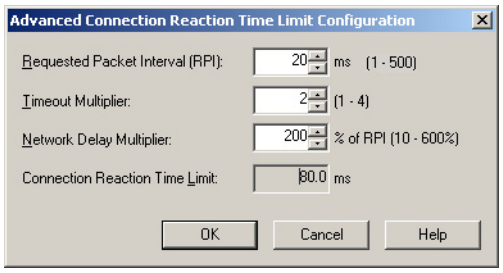
1. In the configuration tree, right-click Controller Tags and choose Edit tags.
2. In the Tag Editor, right-click the name of the tag and choose Edit Properties.
3. Click Connection.



4. Click the Safety tab.



5. Click Advanced to view or edit the current settings.



See the GuardLogix 5570 Controllers User Manual, publication 1756-UM022 for more information.

Checklists for GuardLogix Safety Applications

The checklists in this appendix are required to plan, program, and startup a SIL 3-certified GuardLogix application. They can be used as planning guides and during project verification testing. If used as planning guides, the checklists can be saved as a record of the plan.

The checklists on the following pages provide a sample of safety considerations and are not intended to be a complete list of items to verify. Your particular safety application can have additional safety requirements, for which we have provided space in the checklists.

TIP Make copies of the checklists and keep these pages for future use.

Checklist for GuardLogix Controller System

Checklist for GuardLogix System				
Company				
Site				
Safety Function Definition				
Number	**System Requirements**	**Fulfilled**		**Comment**
		Yes	**No**	
1	Are you using only the components that are listed in SIL 3-certified GuardLogix Components on page 16 and on the http://www.rockwellautomation.com/products/certification/safety/ site, with the corresponding firmware release?	☐	☐	
2	Have you calculated the system's safety response time for each safety chain?	☐	☐	
3	Does the system's response time include both the user-defined safety-task program watchdog (software watchdog) time and the safety task rate/period?	☐	☐	
4	Is the system response time in proper relation to the process tolerance time?	☐	☐	
5	Have probability (PFD/PFH) values been calculated according to the system's configuration?	☐	☐	
6	Have you performed all appropriate project verification tests?	☐	☐	
7	Have you determined how your system will handle faults?	☐	☐	
8	Does each network in the safety system have a unique SNN?	☐	☐	
9	Is each CIP Safety device configured with the correct SNN?	☐	☐	
10	Have you generated a safety task signature?	☐	☐	
11	Have you uploaded and recorded the safety task signature for future comparison?	☐	☐	
12	After a download, have you verified that the safety task signature in the controller matches the recorded safety task signature?	☐	☐	
13	Do you have an alternate mechanism in place to preserve the safety integrity of the system when making online edits?	☐	☐	
14	Have you considered the checklists for using SIL inputs and outputs, which are listed on pages 89 and 90?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

Checklist for Safety Inputs

For programming or startup, an individual checklist can be completed for every SIL input channel in a system. This method is the only way to make sure that the requirements are fully and clearly implemented. This checklist can also be used as documentation on the connection of external wiring to the application program.

Input Checklist for GuardLogix System				
Company				
Site				
Safety Function Definition				
SIL Input Channels				
Number	**Input Device Requirements**	**Fulfilled**		**Comment**
		Yes	**No**	
1	Have you followed installation instructions and precautions to conform to applicable safety standards?	☐	☐	
2	Have you performed project verification tests on the system and devices?	☐	☐	
3	Are control, diagnostics, and alarm functions performed in sequence in application logic?	☐	☐	
4	Have you uploaded and compared the configuration of each device to the configuration sent by configuration tool?	☐	☐	
5	Are devices wired in compliance with PLe/Cat. 4 according to ISO 13849-1?(1)	☐	☐	
6	Have you verified that the electrical specifications of the sensor and input are compatible?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

(1) For information on how to wire your CIP Safety I/O device, refer to the product documentation for your specific device.

Checklist for Safety Outputs

For programming or startup, an individual requirement checklist must be completed for every SIL output channel in a system. This method is the only way to make sure that the requirements are fully and clearly implemented. This checklist can also be used as documentation on the connection of external wiring to the application program.

Output Checklist for GuardLogix System				
Company				
Site				
Safety Function Definition				
SIL Output Channels				
Number	**Output Device Requirements**	**Fulfilled**		**Comment**
		Yes	**No**	
1	Have you followed installation instructions and precautions to conform to applicable safety standards?	☐	☐	
2	Have you performed project verification tests on the devices?	☐	☐	
3	Have you uploaded and compared the configuration of each device to the configuration sent by configuration tool?	☐	☐	
4	Have you verified that test outputs are not used as safety outputs?	☐	☐	
5	Are devices wired in compliance with PLe/Cat. 4 according to ISO 13849-1?(1)	☐	☐	
6	Have you verified that the electrical specifications of the output and the actuator are compatible?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

(1) For information on how to wire your safety I/O device, refer to the product documentation for your specific device.

Checklist for Developing a Safety Application Program

Use the following checklist to help maintain safety when create or modify a safety application program.

Checklist for GuardLogix Application Program Development				
Company				
Site				
Project Definition				
Number	**Application Program Requirements**	**Fulfilled**		**Comment**
		Yes	**No**	
1	Are you using version 21 or later of Logix Designer application, the GuardLogix system programming tool?	☐	☐	
2	Were the programming guidelines in Chapter 6 followed during creation of the safety application program?	☐	☐	
3	Does the safety application program contain only relay ladder logic?	☐	☐	
4	Does the safety application program contain only those instructions that are listed in Appendix A as suitable for safety application programming?	☐	☐	
5	Does the safety application program clearly differentiate between safety and standard tags?	☐	☐	
6	Are only safety tags used for safety routines?	☐	☐	
7	Have you verified that safety routines do not attempt to read from or write to standard tags?	☐	☐	
8	Have you verified that no safety tags are aliased to standard tags and vice versa?	☐	☐	
9	Is each safety output tag correctly configured and connected to a physical output channel?	☐	☐	
10	Have you verified that all mapped tags have been conditioned in safety application logic?	☐	☐	
11	Have you defined the process parameters that are monitored by fault routines?	☐	☐	
12	Have you sealed any safety Add-On Instructions with an instruction signature and recorded the safety instruction signature?	☐	☐	
13	Has the program been reviewed by an independent safety reviewer (if required)?	☐	☐	
14	Has the review been documented and signed?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

Notes:

GuardLogix Systems Safety Data

The following examples show probability of failure on demand (PFD) and probability of failure per hour (PFH) values for GuardLogix 1oo2 SIL 3 systems that use Guard I/O modules.

Mission time for GuardLogix controllers and Guard I/O modules is 20 years.

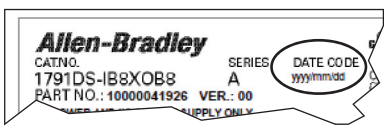
PFD Values

Table 14 - Calculated PFD by Proof Test Interval

Cat. No.	Description	Calculated PFD			
		2 Years (17,520 hours)	5 Years (43,800 hours)	10 Years (87,600 hours)	20 Years (175,200 hours)
1756-L7xS and 1756-L7SP	GuardLogix controller	5.7E-06	1.5E-05	3.5E-05	8.9E-05
1756-L73SXT and 1756-L7SPXT	GuardLogix XT controller	5.7E-06	1.5E-05	3.5E-05	8.9E-05
1791DS-IB12	CIP Safety 12-point input module	4.73E-07	1.18E-06	2.35E-06	4.71E-06(2)
1791DS-IB16	CIP Safety 16-point input module	4.11E-06	1.03E-05	2.06E-05	4.11E-05
1791DS-IB8XOB8	CIP Safety 8-point input/ 8-point output module	4.73E-07	1.18E-06	2.35E-06	4.71E-06(2)
1791DS-IB4XOW4	CIP Safety 4-point input/4-point relay output module	2.21E-05	7.05E-05	1.92E-04	5.88E-04(2)
1791DS-IB8XOBV4	CIP Safety 8-point input/4 bi-polar output module	4.16E-06	1.04E-05	2.08E-05	4.16E-05
1732DS-IB8XOBV4					
1732DS-IB8	CIP Safety 8-point input module	4.11E-06	1.03E-05	2.06E-05	4.11E-05
1791ES-IB16	CIP Safety 16-point input module	4.13E-06	1.03E-05	2.06E-05	—
1791ES-IB8XOBV4	CIP Safety 8-point input/4 bi-polar output module	4.17E-06	1.04E-05	2.09E-05	—
1734-IB8S, series A	CIP Safety 8-point input module	4.23E-06	1.06E-05	2.11E-05	4.23-05
1734-IB8S, series B(1)	CIP Safety 8-point input module	4.36E-06	1.09E-05	2.18E-05	4.36E-05
1734-OB8S, series A	CIP Safety 8-point output module	4.27E-06	1.07E-05	2.13E-05	4.27E-05
1734-OB8S, series B	CIP Safety 8-point output module	4.32E-06	1.08E-05	2.16E-05	4.32E-05
1734-IE4S	CIP Safety 4-point analog input module, single-channel operation	4.7E-07	1.2E-06	2.4E-06	4.8E-06
1734-IE4S	CIP Safety 4-point analog input module, dual-channel operation	3.2E-07	8.1E-07	1.6E-06	3.3E-06

(1) This data is for single and dual channel operation.

(2) The 20-year PFD data for this product applies only to product with a manufacture date code of 2009/01/01 (January 1, 2009) or later. See the product label for the date code.



PFH Values

The data below applies to proof test intervals up to and including 20 years.

Table 15 - PFH Calculation

Cat. No.	Description	PFH (1/Hour)
1756-L7xS and 1756-L7SP	GuardLogix controller	1.2E-09
1756-L7xSXT and 1756-L7SPXT	GuardLogix-XT controller	1.2E-09
1791DS-IB12	CIP Safety 12-point input module	5.77E-11(1)
1791DS-IB16	CIP Safety 16-point input module	4.96E-10
1791DS-IB8XOB8	CIP Safety 8-point input/ 8-point output module	5.77E-11(1)
1791DS-IB4XOW4	CIP Safety 4-point input/4-point relay output module	9.03E-09(1)
1791DS-IB8XOBV4	CIP Safety 8-point input/4 bi-polar output module	5.02E-10
1732DS-IB8XOBV4		
1732DS-IB8	CIP Safety 8-point input module	4.96E-10
1791ES-IB16	CIP Safety 16-point input module	4.98E-10
1791ES-IB8XOBV4	CIP Safety 8-point input/4 bi-polar output module	5.04E-10
1734-IB8S, series A	CIP Safety 8-point input module	5.10E-10
1734-IB8S, series B	CIP Safety 8-point input module	5.27E-10
1734-OB8S, series A	CIP Safety 8-point output module	5.14E-10
1734-OB8S, series B	CIP Safety 8-point output module	5.20E-10
1734-IE4S	CIP Safety 4-point analog input module, single-channel operation CIP Safety 4-point analog input module, dual-channel operation	5.6E-11 3.9E-11

(1) The PFH data for this product applies only to product with a manufacture date code of 2009/01/01 (January 1, 2009) or later. See the product label for the date code.

RSLogix 5000 Software, Version 14 and Later, Safety Application Instructions

De-energize to Trip System

When using instructions from RSLogix 5000 software, version 14, safety application instructions, all inputs and outputs are set to zero when a fault is detected. As a result, any inputs that are monitored by one of the diverse input instructions (Diverse Inputs or Two-hand Run Station) should have normally-closed inputs that are conditioned by logic similar to the logic in Rung 4 of Ladder Logic Example 2 and Ladder Logic Example 3 on pages 98 and 99. The exact logic that is required is both application and input-device dependent. However, the logic must create a safety state of 1 for the normally-closed input of the diverse input instructions.

Use Connection Status Data to Initiate a Fault Programmatically

The following diagrams provide examples of the application logic that is required to latch and reset I/O failures. The examples show the logic necessary for input only modules, and for input and output combination modules. The examples use the Combined Status feature of the I/O modules, which presents the status of all input channels in one Boolean variable. Another Boolean variable represents the status of all output channels. This approach reduces the amount of I/O conditioning logic that is required and forces the logic to shut down all input or output channels on the affected module.

Use the Input Fault Latch and Reset Flow Chart on page 96 to determine which rungs of logic are required for different application situations. Ladder Logic Example 1 shows logic that overwrites the actual input-tag variables while a fault condition exists. If the actual input state is required for troubleshooting while the input failure is latched, use the logic shown in Ladder Logic Example 2. This logic uses internal tags that represent the inputs to be used in the application logic. While the input failure is latched, the internal tags are set to their safety state. While the input failure is not latched, the actual input values are copied to the internal tags.

Use the Output Fault Latch and Reset Flowchart to determine which rungs of application logic in Ladder Logic Example 3 on page 99 are required.

Figure 22 - Input Fault Latch and Reset Flow Chart

Figure 23 - Ladder Logic Example 1

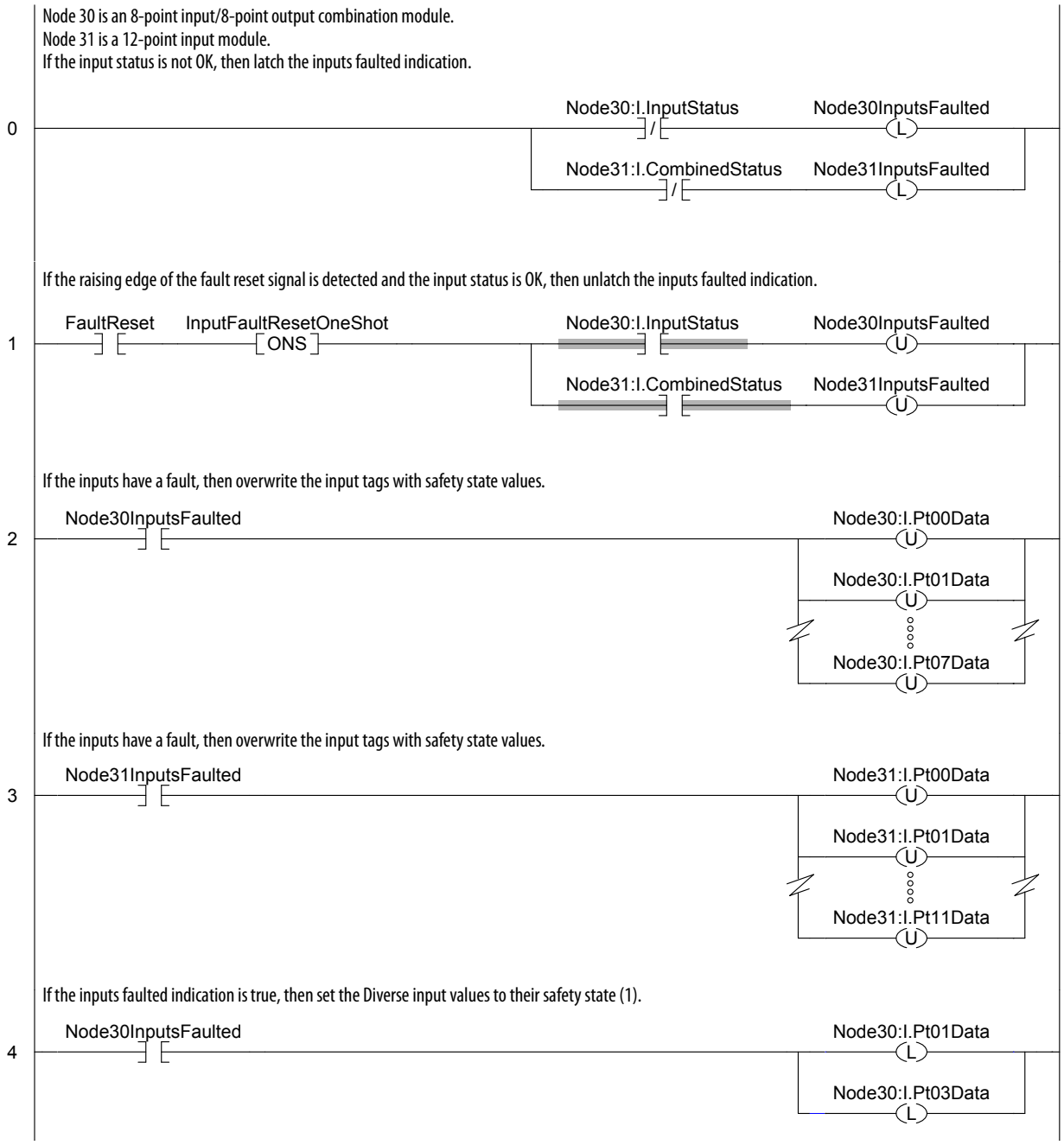


Figure 24 - Ladder Logic Example 2

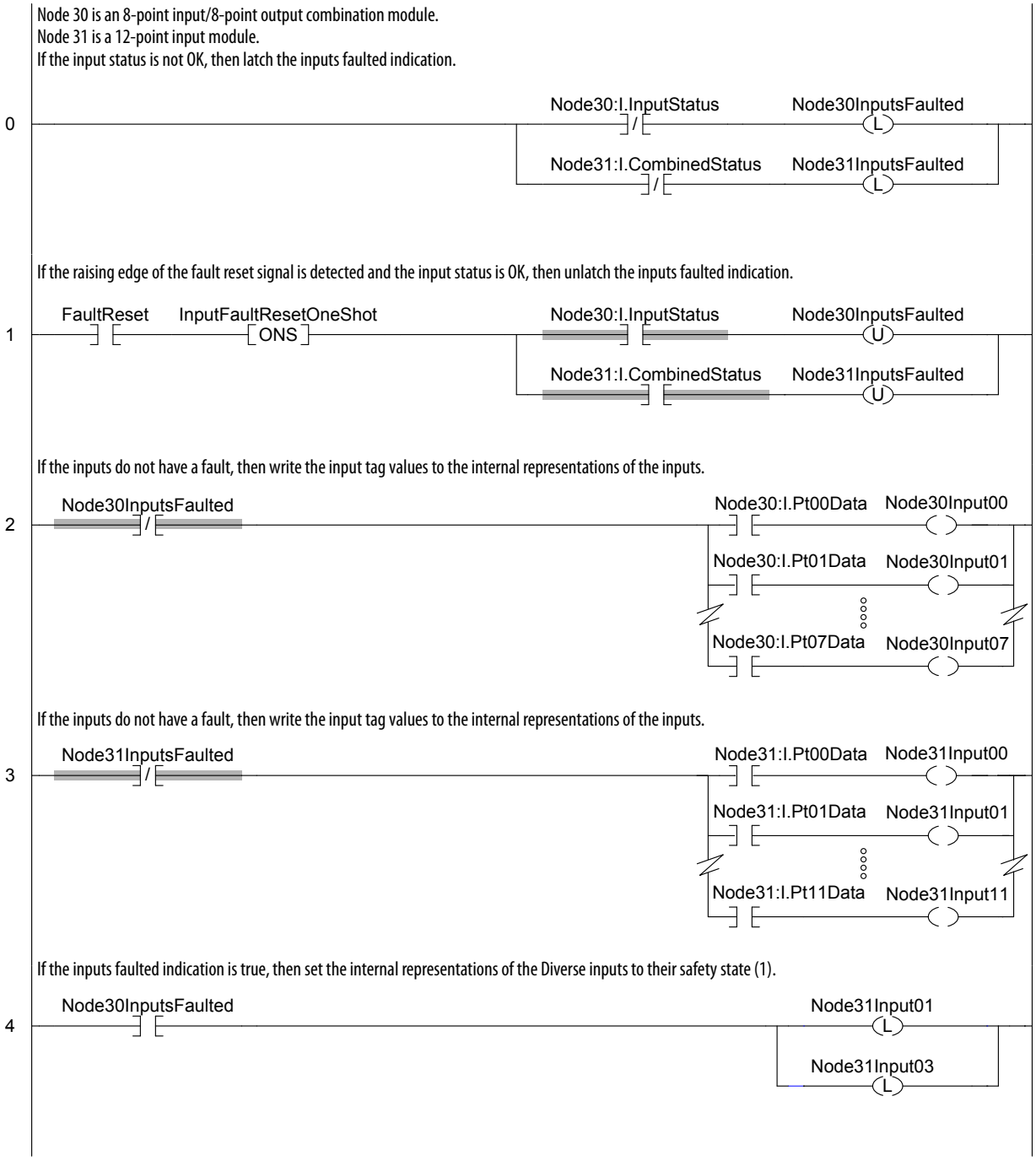


Figure 25 - Output Fault Latch and Reset Flowchart

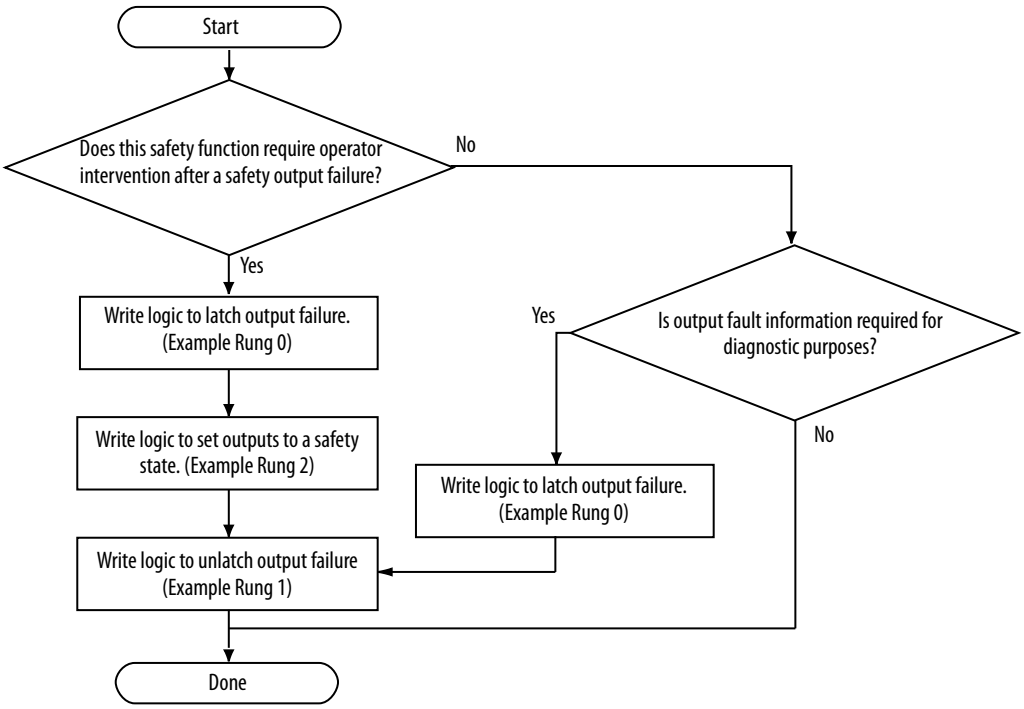
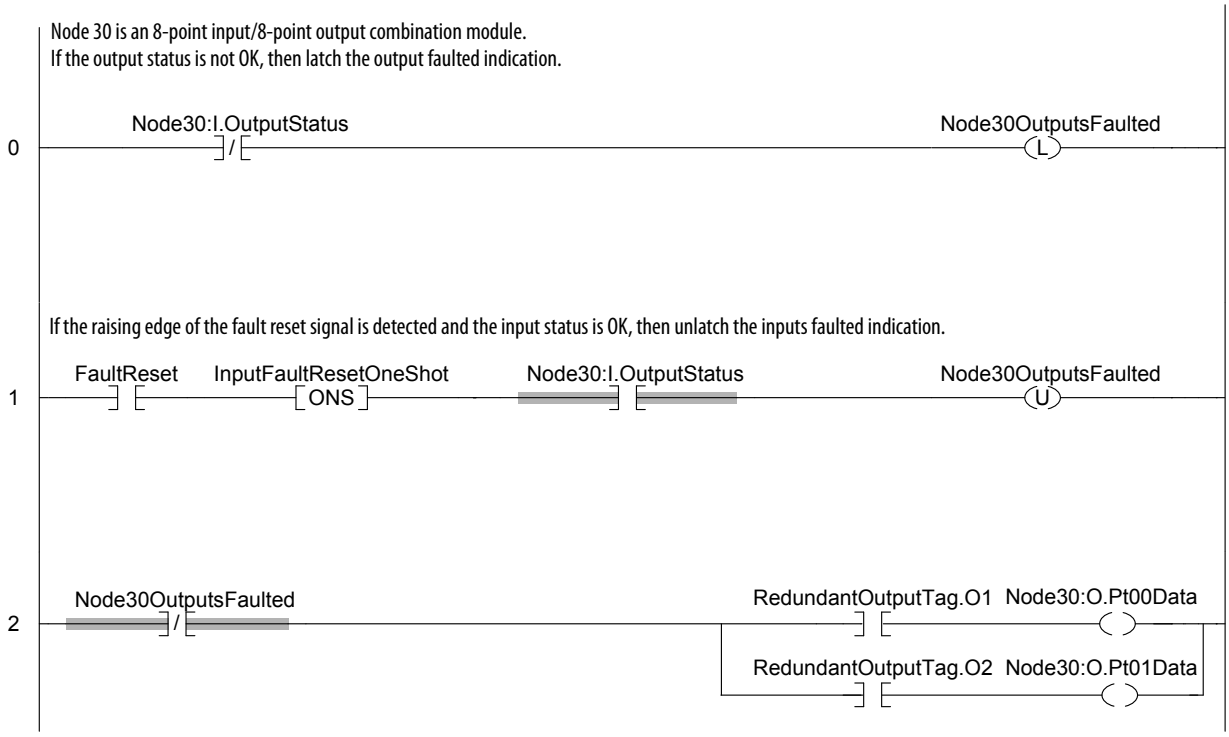


Figure 26 - Ladder Logic Example 3



Notes:

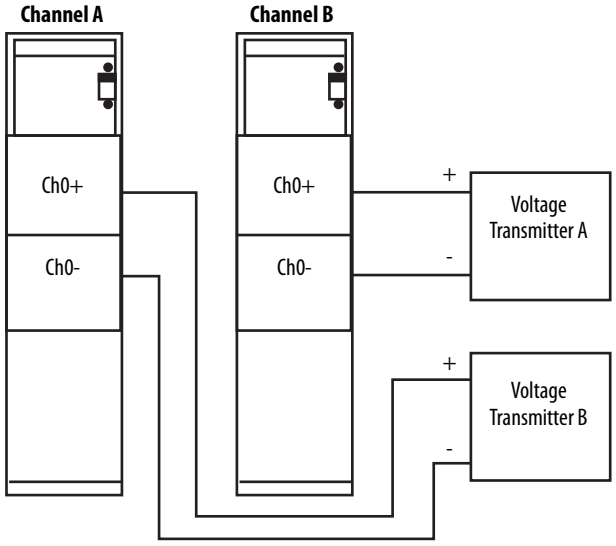
Using 1794 FLEX I/O Modules and 1756 SIL 2 Inputs and Outputs with 1756 GuardLogix Controllers to Comply with EN 50156

Dual channel configuration is required for compliance in certain safety-related applications, including burner-related safety functions. These examples provide guidelines for satisfying EN50156 SIL 2 dual channel requirements with 1- and 2-year proof test intervals.

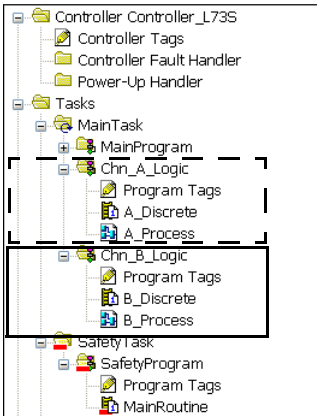
SIL 2 Dual Channel Inputs (standard side of GuardLogix controllers)

You must implement clear and easily identifiable separation between both input channels and adhere to all existing SIL 2 requirements as defined in Using ControlLogix in SIL 2 Applications, publication 1756-RM001.

Figure 27 - SIL 2 Dual Channel Inputs Example F



SIL 2 Input Data



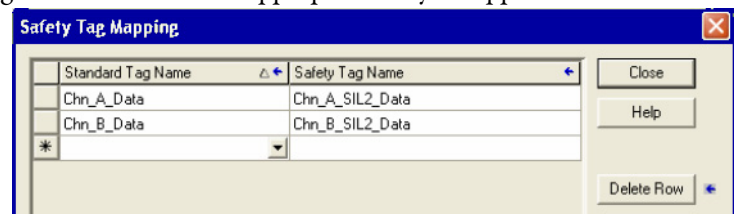
Always keep channel A and channel B input data separate. This example illustrates one method to separate channel A and channel B data in your application.

Follow all rules for 1756 I/O modules and 1794 FLEX™ I/O modules as defined in the Using ControlLogix in SIL 2 Applications Safety Reference Manual, publication 1756-RM001.

IMPORTANT Do not perform safety-specific functions within these routines. Safety evaluation must be handled within the 1756 GuardLogix safety task.

Transferring SIL 2 Data Into the Safety Task

To transfer channel A and channel B SIL 2 safety data into the GuardLogix safety task, use the safety-tag mapping functionality in the Logix Designer application. The tag names that are used here are for example purposes. Implement and follow naming conventions that are appropriate for your application.



TIP To use the safety-tag mapping feature, select Map Safety Tags from the Logic menu in the Logix Designer application.

SIL 2 Outputs Using SIL 3 Guard I/O Output Modules

Follow these guidelines for SIL 2 outputs:

- Guard I/O output modules that are used for SIL 2 safety outputs must be configured for dual channel operation.
- All Guard I/O output modules are approved for use in SIL 2 applications.
  - 1732DS-IB8XOBV4
  - 1791ES-IB8XOBV4
  - 1791DS-IB8XOBV4, 1791ES-IB8XOBV4
  - 1791DS-IB4XOW4
  - 1791DS-IB8XOB8
  - 1734-OB8S

SIL 2 Outputs Using 1756 or 1794 SIL 2 Output Modules

When using these SIL 2-rated output modules, you are required to configure your SIL 2 safety outputs as GuardLogix-produced safety tags to comply with the dual channel requirements of EN 50156.

Create produced safety tags with the SIL 2 outputs that your application requires. GuardLogix produced/consumed safety tags require the first member to be allocated for diagnostics. The first member of a produced/consumed safety connection must be a data type called CONNECTION_STATUS. This example shows a SIL 2 tag with two INT and two BOOL members. Use these SIL 2 safety tags to control the 1756 or 1794 SIL 2 outputs directly.

Name	Alias For	Base Tag	Data Type	Class	Description	External Access	Constant	Style
SIL2_Outputs			SIL_2_Produced	Safety		Read/Write	☐	
SIL2_Outputs.Connection_Status			CONNECTION_STA	Safety		Read/Write		
SIL2_Outputs.SIL2_TempA			INT	Safety		Read/Write		Decimal
SIL2_Outputs.SIL2_TempB			INT	Safety		Read/Write		Decimal
SIL2_Outputs.SIL2_Valve1			BOOL	Safety		Read/Write		Binary
SIL2_Outputs.SIL2_Valve2			BOOL	Safety		Read/Write		Binary

TIP In this example, a consumer for the produced tag is not shown. The connection status shows a fault if you don't configure a consumer. However, in this type of configuration, you are not required to monitor the connection status of the produced tag so the fault is not a concern.

Follow all rules for 1756 I/O modules and 1794 FLEX I/O modules as defined in the Using ControlLogix in SIL 2 Applications Safety Reference Manual, publication 1756-RM001.

Safety Functions Within the 1756 GuardLogix Safety Task

Follow these guidelines for using SIL 2 and SIL 3 safety functions within the safety task:

- All available safety application instructions can be used.
- SIL CL3 safety input modules (that is, Guard I/O modules) can be used with single-channel configuration for SIL 2 safety functions.
- Use of the safety task signature and safety-locking the application is recommended.

IMPORTANT You must not use SIL 2 data to control a SIL 3 output directly.

The following terms and abbreviations are used throughout this manual. For definitions of terms that are not listed here, refer to the Allen-Bradley Industrial Automation Glossary, publication AG-7.1.

add-on instruction An instruction that you create as an add-on to the Logix instruction set. Once defined, an Add-On Instruction can be used like any other Logix instruction and can be used across various projects. An Add-On Instruction is composed of parameters, local tags, logic routine, and optional scan-mode routines.

assemble edits You assemble edits when you have made online edit changes to the controller program and want the changes to become permanent because you can test, untest, or cancel the edits.

cancel edits Action that is taken to reject any unassembled online edit changes.

CIP Safety protocol A network communication method that is designed and certified for transport of data with high integrity.

configuration signature A unique number that identifies the configuration of a device. The configuration signature is composed of an ID number, date, and time.

instruction signature The instruction signature consists of an ID number and date/timestamp that identifies the contents of the Add-On Instruction definition at a given point in time.

nonrecoverable controller fault A fault that forces all processing to be ended and requires controller power to be cycled from off to on. The user program is not preserved and must be re-downloaded.

nonrecoverable safety fault A fault, which even though properly handled by the fault handling mechanisms that are provided by the safety controller and implemented by the user, ends all safety task processing, and requires external user action to restart the safety task.

online Situation where you are monitoring/modifying the program in the controller.

overlap When a task (periodic or event) is triggered while the task is still executing from the previous trigger.

partnership The primary controller and safety partner must both be present, and the hardware and firmware must be compatible for partnership to be established.

pending edit A change to a routine that has been made in the Logix Designer application, but has not yet been communicated to the controller by accepting the edit.

periodic task A task that is triggered by the operating system at a repetitive period. Whenever the time expires, the task is triggered and its programs are executed. Data and outputs that are established by the programs in the task retain their values until the next execution of the task or until they are manipulated by another task. Periodic tasks always interrupt the continuous task.

primary controller The processor in a dual-processor controller that performs standard controller functionality and communicates with the safety partner to perform safety-related functions.

recoverable fault A fault, which when properly handled by implementing the fault handling mechanisms that are provided by the controller, does not force user logic execution to be ended.

requested packet interval (RPI) When communicating over a network, this value is the maximum amount of time between subsequent production of input data.

routine A set of logic instructions in one programming language, such as a ladder diagram. Routines provide executable code for the project in a controller. Each program has a main routine. You can also specify optional routines.

safety add-on instruction An Add-On Instruction that can use safety application instructions. In addition to the instruction signature used for high-integrity Add-On Instructions, safety Add-On Instructions feature a SIL 3 safety instruction signature for use in safety-related functions.

safety application instructions Safety Instructions that provide safety-related functionality. They have been certified to SIL 3 for use in safety routines.

safety component Any object, task, program, routine, tag, or module that is marked as a safety-related item.

safety instruction signature The safety instruction signature is an ID number that identifies the execution characteristics of the safety Add-On Instruction. It is used to verify the integrity of the safety Add-On Instruction during downloads to the controller.

safety I/O Safety I/O has most of the attributes of standard I/O except it features mechanisms that are certified to SIL 3 for data integrity.

safety network number (SNN) Uniquely identifies a network across all networks in the safety system. The end user is responsible is responsible for assigning a unique number for each safety network or safety subnet within a system. The safety network number constitutes part of the Unique Node Identifier (UNID).

safety partner The processor in a dual-processor controller that works with the primary controller to perform safety-related functions.

safety program A safety program has all the attributes of a standard program, except that it can be scheduled only in a safety task. The safety program consists of zero or more safety routines. It cannot contain standard routines or standard tags.

safety routine A safety routine has all the attributes of a standard routine except that it is valid only in a safety program and that it consists of one or more instructions suitable for safety applications. (See Appendix A for a list of Safety Application Instructions and standard Logix Instructions that can be used in safety routine logic.)

safety tags A safety tag has all the attributes of a standard tag except that the GuardLogix controller provides mechanisms that are certified to SIL 3 to help protect the integrity of their associated data. They can be program-scoped or controller-scoped.

safety task A safety task has all the attributes of a standard task except that it is valid only in a GuardLogix controller and that it can schedule only safety programs. Only one safety task can exist in a GuardLogix controller. The safety task must be a periodic/timed task.

safety task period The period at which the safety task executes.

safety task reaction time The sum of the safety task period plus the safety task watchdog. This time is the worst case delay from any input change that is presented to the GuardLogix controller until the processed output is available to the producing connection.

safety task signature A value, which is calculated by the firmware, that uniquely represents the logic and configuration of the safety system. It is used to verify the integrity of the safety application program during downloads to the controller.

safety task watchdog The maximum time that is allowed from the start of safety task execution to its completion. Exceeding the safety task Watchdog triggers a nonrecoverable safety fault.

standard component Any object, task, tag, program, and so on, that is **not** marked as being a safety-related item.

standard controller As used in this document, standard controller refers generically to a ControlLogix controller.

symbolic addressing A method of addressing that provides an ASCII interpretation of the tag name.

system reaction time The worst case time from a safety-related event as input to the system or as a fault within the system, until the time that the system is in the safe state. System Reaction Time includes sensor and activator Reaction Times and the Controller Reaction Time.

task A scheduling mechanism for executing a program. A task provides scheduling and priority information for a set of one or more programs that execute based on a certain criteria. Once a task is triggered (activated), all programs assigned (scheduled) to the task execute in the order in which they are displayed in the controller organizer.

timeout multiplier This value determines the number of messages that can be lost before declaring a connection error.

valid connection Safety connection is open and active, with no errors.

Numerics

A

B

C

D

E

F

G

T

U

W

X

Notes:

Rockwell Automation Support

Rockwell Automation provides technical information on the Web to assist you in using its products. At http://www.rockwellautomation.com/support you can find technical and application notes, sample code, and links to software service packs. You can also visit our Support Center at https://rockwellautomation.custhelp.com/ for software updates, support chats and forums, technical information, FAQs, and to sign up for product notification updates.

In addition, we offer multiple support programs for installation, configuration, and troubleshooting. For more information, contact your local distributor or Rockwell Automation representative, or visit http://www.rockwellautomation.com/services/online-phone.

Installation Assistance

If you experience a problem within the first 24 hours of installation, review the information that is contained in this manual. You can contact Customer Support for initial help in getting your product up and running.

United States or Canada	1.440.646.3434
Outside United States or Canada	Use the Worldwide Locator at http://www.rockwellautomation.com/rockwellautomation/support/overview.page, or contact your local Rockwell Automation representative.

New Product Satisfaction Return

Rockwell Automation tests all of its products to help ensure that they are fully operational when shipped from the manufacturing facility. However, if your product is not functioning and needs to be returned, follow these procedures.

United States	Contact your distributor. You must provide a Customer Support case number (call the phone number above to obtain one) to your distributor to complete the return process.
Outside United States	Please contact your local Rockwell Automation representative for the return procedure.

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete this form, publication RA-DU002, available at http://www.rockwellautomation.com/literature/.

Rockwell Automation maintains current product environmental information on its website at http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1756-RM099C-EN-P - May 2015
Supersedes Publication 1756-RM099B-EN-P - November 2014